Troubleshooting

This chapter offers troubleshooting steps to help solve high-level problems while operating CTM or CTM GateWay. Follow the troubleshooting procedures described in this chapter before contacting Cisco technical support.

This chapter includes the following troubleshooting information:

- J.1 Overview, page J-1
- J.2 Server Problems, page J-2
- J.3 Client Connectivity Problems, page J-11
- J.4 Client Operational Problems, page J-13
- J.5 Client Debug Messages, page J-20
- J.6 CTM GateWay/TL1 Problems, page J-21
- J.7 CTM GateWay/CORBA Problems, page J-21
- J.8 Cisco CRS-1 and Catalyst 6509 Problems, page J-22
- J.9 XR 12000 Problems, page J-31
- J.10 Problems with MGX Voice Gateway Devices, page J-34

Note For information about troubleshooting CiscoView problems, see I.9 Troubleshooting, page I-6 in Appendix I, "Using CiscoView to Configure and Monitor ONS 15501, ONS 15530, and ONS 15540 NEs."

J.1 Overview

Troubleshooting involves:

1. Identifying the source of the problem—Which devices, links, interfaces, hosts, or applications have the problem?
2. Locating the problem on the network—On what VLAN, subnet, or segment is the problem occurring?
3. Comparing current network performance against an established baseline—Is the performance better or worse?
4. Finding out when the problem started—When did you first see the problem? Is it recurring?
5. Determining the extent of the problem—How widespread is the problem? Is it getting worse?

Note This chapter assumes that the server is installed under the default /opt/CiscoTransportManagerServer directory and the client is installed under the default /opt/CiscoTransportManagerClient (Solaris) or C:\Cisco\TransportManagerClient directory (Windows). If a directory other than the default installation directory is specified, replace the default path with the installed path.

J.2 Server Problems

This section describes troubleshooting procedures for CTM server-related problems.

Note Log in as the root user on the Solaris workstation where the CTM server is installed to perform any operations on the Solaris workstation.

J.2.1 Conditions that Affect CTM Server Performance

The "System Requirements" chapter in the *Cisco Transport Manager Installation Guide* lists server, CPU, CPU speed, disk space, and RAM requirements for different types of CTM installations. These requirements are derived from guidelines based on scalability simulation testing.

Actual CTM server performance varies for each customer and is affected by:

- The total number of NEs actively managed by CTM
- The number of NE-related services (including northbound services) running on the server
- The rate of circuit provisioning and the methods used for provisioning
- The rate of network growth (for example, adding 50 NEs to CTM at once)
- The rate of configuration change updates received from the NEs
- The number of circuits provisioned with no signals that generate threshold crossing alerts (TCAs)
- The number of unacknowledged alarms in the CTM database
- The rate of alarm bursts received from the NEs
- The actual number of circuits provisioned in the CTM database

The following conditions might indicate that your CTM installation is near or at capacity:

- Your daily CPU utilization is consistently above 80%
- You experience loss of connectivity (LOC) to 1% to 5% of nodes at random
- Your RAM usage is 100% or your system swaps frequently
- You receive many configuration updates from the NEs
- Your system experiences high Java garbage collection time

Note The Java garbage collection time is determined by engineering after analyzing your CPU utilization data.

If you are experiencing any of these conditions, contact your account representative. Your account representative can engage Cisco's Advanced Services team to audit your CTM server and recommend a higher-capacity server and resources.

J.2.2 CTM Server Does Not Respond

Step 1 Log in as the root user on the Solaris workstation where the CTM server is installed.

Step 2 Enter the following command to view the status of the CTM server processes:

```
showctm
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as nonroot, enter the following command:

```
sudo showctm
```

If there is a line containing /CTMServer, the CTM server is running.

If there is no line containing /CTMServer, the CTM server is not running. Proceed to Step 3.

Note You can also check the ctmop.log file in /opt/CiscoTransportManagerServer/log to determine if the server was stopped by another user or if it stopped abnormally. If it stopped abnormally, proceed to Step 3.

Step 3 Run the **getinfo.sh** CTM server tool and send the data to Cisco technical support for analysis.

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as nonroot, enter the following command:

```
sudo getinfo.sh
```

Step 4 Start the CTM server by using the ctms-start script in the /opt/CiscoTransportManagerServer/bin directory.

a. Log in as the root user.

b. Change the directory to /opt/CiscoTransportManagerServer/bin and enter the following command:

```
ctms-start
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as nonroot, enter the following command:

```
sudo ctms-start
```

If the preceding procedure does not solve the problem, complete the following steps:

Step 1 Verify that the /opt/CiscoTransportManagerServer/cfg/CTMServer.cfg file is not corrupted. The file should contain the db-config-mode = auto parameter in the [database] section. If the entry is missing, the CTM server configuration file is corrupt. Reinstall the CTM server.

Step 2 Verify that the first entry in the /var/opt/oracle/oratab file looks similar to CTM6_0:/oraclesw9i/product/9.2:Y. If this entry is missing, the Oracle database might not be installed. The Oracle database is a prerequisite for installing the CTM server.

J.2.3 Cannot Connect to the CTM Server

Step 1 Ping the server's IP address from the client PC or workstation.

Step 2 If the ping fails, resolve the IP connectivity problem and try again.

Step 3 Telnet to the server and log in as the root user.

Step 4 Enter the following command to verify that CTM is running:

```
showctm
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as nonroot, enter the following command:

```
sudo showctm
```

Step 5 The server should have at least the following four processes running:

```
root 3778 0.1 0.1567 9592 ? S 16:57:36 0:00 /opt/CiscoTransportManagerServer/bin/CTMServer
root 3771 0.1 0.4 6208 pts/1 S 16:57:34 0:00
/opt/CiscoTransportManagerServer/bin/CTMServer
root 3876 0.5 0.6129464 8648 ? R 16:58:12 SnmpTrapService
root 3798 26.8 4.115732060968 ? S 16:57:37 0:29 SMService
```

Step 6 Manually stop the server if you see fewer than four processes running. Enter the following command:

```
ctms-stop
```

Step 7 If you changed the server IP address, verify that the configuration files shown in Table 4-13 on page 4-44 have been updated. See 4.4.2 Updating the Configuration Files After Changing the CTM Server IP Address, page 4-44.

Step 8 Verify that the Oracle database is accepting connections:

a. Enter the following command to log in as the Oracle user:

```
su-oracle
```

b. Enter the following command to open an SQL*Plus session:

```
omu-u60-3% sqlplus ctmanager/ctm123!
```

Step 9 Reboot the server if you receive another error message and the SQL prompt does not appear. Wait enough time for the server to boot up and try to run the client. The SQL prompt indicates that the Oracle database is running and accepting connections.

Step 10 Enter the following commands to manually restart CTM:

```
SQL> exit
omu-u60-3% exit
omu-u60-3% logout
ctms-start
```

If you do not have root user privileges but you belong to the UNIX group that can use sudo functionality to run commands as nonroot, enter the following command:

```
sudo ctms-start
```

Step 11 Wait for 5 minutes and run the client.

J.2.4 NE Connection State Is Listed as Unavailable

If the connection state of an NE is listed as Unavailable in the Domain Explorer window, a connectivity or configuration problem exists. Wait 5 to 10 minutes after adding the NE to the CTM domain; then, complete the following steps:

Step 1 To see the NE IP address, select the NE in the Domain Explorer window. The Address tab of the Network Element Properties pane lists the IP address of the selected NE.

Step 2 From the CTM server, enter the following command to verify connectivity between the CTM server and the NE:

```
ping <IP_address>
```

Step 3 If the ping fails, a physical or configuration problem exists in the data communications network (DCN).

a. If connectivity existed earlier:

- If there were no configuration changes made to any routers in the DCN or to the CTM server, the problem is a physical problem.
- If the configuration was changed, the change might have introduced problems. Verify the changed configuration.

b. If connectivity was never established:

- Verify that there are no problems on the physical level.
- Verify the DCN configuration.

Step 4 If the ping succeeds, verify that the NE software version is listed in the Supported NE Table. See 4.3.7 Adding a New NE Software Version to the CTM Domain, page 4-37.

Step 5 For ONS 15501, ONS 15530, and ONS 15540 NEs, SNMP read and write community strings must be set up properly on each NE. The running configuration on each NE should contain entries similar to the following example:

```
snmp-server community public RO
snmp-server community private RW
```

The community strings configured on the server should match the strings configured on the NE. For information on configuring community strings in CTM for ONS 15501, ONS 15530, and ONS 15540 NEs, see 3.5.1.4 Prerequisites for Adding ONS 15501, ONS 15530, and ONS 15540 NEs, page 3-10.

J.2.5 Launching Tables Results in Database Errors

If the Oracle database or Oracle listener that CTM is using is down, launching tables will generate database errors. To troubleshoot table launching errors:

Step 1 Log in as the Oracle user and enter the following command:

```
sqlplus ctmanager/ctm123!
```

If the login is successful, an SQL> prompt appears, which indicates that the Oracle database has been installed and the database server is up and running. If login fails, either the Oracle database has not been installed or the database server is not running.

Step 2 To start the Oracle database, log into the Solaris workstation as the Oracle software owner user.

Step 3 Enter the following command at the shell prompt to start the Oracle database:

```
dbstart
```

Step 4 Enter the following command at the shell prompt to start the Oracle listener:

```
lsnrctl start
```

If there are still problems with starting the Oracle database or the Oracle listener, refer to the Oracle documentation or contact Oracle support.

J.2.6 SNMP Traps Are Not Forwarded from NEs

SNMP traps might not be forwarded, either because the trap port is already in use, or because the NE is not properly configured.

J.2.7 Trap Port Is Unavailable

The CTM server requires exclusive access to the SNMP trap port to receive SNMP traps from the NE.

Step 1 To verify that the standard SNMP trap port (number 162) is not being used by another application running on the same Solaris workstation, enter the following command:

```
netstat -a | grep 162
```

If the following line is seen, the SNMP trap port is being used by another application:

```
*.162 Idle
```

Step 2 If the trap port is being used by another application, stop the other application.

J.2.8 Problems with ONS 15530 and ONS 15540 Configuration

ONS 15530 and ONS 15540 NEs must be properly configured to send traps to the server.

Step 1 The running configuration on the NE should contain entries similar to the following example:

```
snmp-server enable traps snmp authentication warmstart
snmp-server enable traps bgp
snmp-server enable traps oscp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps topology throttle-interval 60
snmp-server enable traps optical monitor min-severity not-alarmed
snmp-server enable traps rf
snmp-server enable traps aps
snmp-server enable traps patch
snmp-server enable traps cdl all
snmp-server enable traps alarms
snmp-server enable traps threshold min-severity degrade

snmp-server host 172.20.126.214 version 2c public snmp bgp oscp
config entity fru-ctrl topology optical rf aps patch cdl alarms threshold
```

In this example, the host 172.20.126.214 will receive the specified traps from the NE.

Step 2 You can also run the following commands on the server and device:

a. As the root user, enter the following command on the server:

```
# snoop udp port 162
```

b. On the device, enter the following command to generate a configuration change:

```
wr mem
```

If the device is configured correctly, the **snoop** command reports a configuration change trap.

J.2.9 Performance Monitoring Data Is Not Displayed

Step 1 Use the Domain Explorer NE Properties pane to see if PM collection is disabled for the selected NE.

Step 2 Choose **Administration > Control Panel** and expand **PM Service**. Select the NE type to see if the service status is Active or Not Active.

Step 3 Choose **Administration > Audit Log** to see if PM was ignored for the selected NE.

Step 4 Choose **Administration > Control Panel** and click **PM Service**. Look at the PM Data Storage field. Choose **Optimized** to save only nonzero values in the database. Choosing Optimized requires less space than saving all values, including zero values. If you choose Normal in the PM Data Storage field, the database saves all PM values, including zero values.

Note The Optimized PM data storage feature is available only for CTC-based and ONS 155xx NEs.

Step 5 Choose **Administration > Error Log** to see if there are any critical, major, or minor errors against the PM service.

Step 6 Verify that the NE is reachable during the duration that PM data is collected. If the NE is not reachable, there is an entry in the Audit Log table (**Administration > Audit Log**).

J.2.10 CTC-Based NE Is Not Discovered

Step 1 Verify that the NE is up and running.

Step 2 Verify that the NE IP address and default route are configured correctly.

Step 3 To verify that the NE is running the correct version of system software, open a CTC session to the NE and check the NE software version.

Step 4 Verify that the NE that acts as the gateway NE (GNE) (through which this node is discovered) is added to CTM and is available.

Step 5 Open CTC from the GNE and see if CTC can discover the NE.

J.2.11 CTC-Based NE Is Not Reachable

Step 1 Verify that the NE is up and running.

Step 2 Verify that the NE IP address and default route are correctly configured.

Step 3 Wait for five poll cycles while CTM reestablishes connectivity with the NE.

Step 4 To test IP connectivity to the NE from the CTM server, enter the following command from the Solaris workstation running CTM:

```
ping <NE_IP_address>
```

Step 5 To verify that the NE is running the version of system software supported by CTM, open a CTC session to the NE and check the NE software version.

Step 6 Verify that the username and password that CTM uses to reach the NE exist on the NE.

J.2.12 ONS 15501, ONS 15540, or ONS 15530 Is Not Reachable

Step 1 Enter the following command on the server to verify IP connectivity between the server and the NE:

```
ping <NE_IP_address>
```

Step 2 If the NE is reachable through IP, verify that the correct read community string is configured on the server.

- On the server, choose **Administration > ONS 155XX > ONS 155XX SNMP Settings Table** to view the community strings set in CTM.
- On the NE, enter the following command to view the read community string set on the NE:

```
show run | begin SNMP
```

- In the running configuration, the community strings are shown in entries similar to the following:

```
snmp-server community public RO
snmp-server community private RW
```

  In this example, the read string is *public*, and the read/write string is *private*.

Step 3 If IP connectivity and community strings are verified and the device is still unavailable, check the error log for any errors reported by ONS 155xx NE Service.

J.2.13 Circuits Are Not Displayed

If CTM fails to display some circuits or if the information displayed by CTC and CTM differs, complete the following steps:

Step 1 Wait for two minutes while the CTM server synchronizes with the NE. If the Circuit table is not in autorefresh mode, click the **Refresh Data** tool when the tool flashes.

Step 2 Verify that the Circuit table is opened from either the source or destination NE of the circuit to be viewed.

Step 3 Verify that the NEs that are part of the circuit (source, destination, or drop) are available in CTM.

Step 4 Open another CTC session and compare the circuit information in the newly opened CTC session with the circuit information displayed by CTM.

J.2.14 Circuit State for Monitor Circuits Reads "Duplicate ID"

CTM generates a unique number that is appended to the circuit name to make the monitor circuit name unique. On rare occasions, CTM might create two or more monitor circuits with the same name. The circuit state for these circuits reads "Duplicate ID." This is a known issue that has been tracked as DDTS number CSCdz87566.

When the circuit state reads "Duplicate ID," you cannot see the actual circuit state. In this case, you must change the duplicate name to a unique name, so that you can see the correct circuit state. Use the Modify Circuit wizard to enter a unique name for each monitor circuit.

J.2.15 NE Model Type Appears as Unknown

If an in-service NE is added to the Domain Explorer, but the model type appears as unknown, the software version of the NE might not be prepopulated in the database. In other words, CTM cannot match the NE with a recognizable version.

Use the NE Software Table to add the NE software version string to the CTM database. See 4.3.5 Viewing Software Versions and Restarting the NE with a New Software Image, page 4-35.

J.2.16 Cannot Copy CTC Binary to the CTM Server

If a CTC binary fails to be copied to the CTM server, the <C*TM_install_directory*>/cms/ directory might be missing or write-protected. If the directory is missing, create a cms directory with write-access permissions. Otherwise, change the permissions of the existing cms directory to allow write access.

J.2.17 Memory Backup, Memory Restore, or Software Download Fails

Step 1 In the Domain Explorer window, choose **Administration > Job Monitor**. The Job Monitor table shows the status of the operation. The reason for the failure is shown in the Additional Information column.

Step 2 Return to the Domain Explorer window and choose **Administration > Error Log**. The Error Log table shows information about the backup, memory restore, or download failure.

Step 3 See Appendix H, "Error Messages" for the correct action to take in response to the error.

J.2.18 Memory Autobackup, Software Commit, or Software Revert Fails

Step 1 In the Domain Explorer window, choose **Administration > Audit Log**. The Audit Log table shows the status of the operation.

Step 2 Return to the Domain Explorer window and choose **Administration > Error Log**. The Error Log table shows the reason for the failure.

Step 3 See H.2 CTM Server Error Messages, page H-94 for the correct action to take in response to the error.

J.2.19 The getinfo.sh Script Fails

You might experience a problem where the getinfo.sh script fails with the following error:

"Error: permission denied while running 'rsh.' Check the environment and make sure the root is permitted to run .rsh on host <*IP_address*>."

This problem occurs because the getinfo.sh script does not run unless an entry is made in the /.rhosts file. This problem occurs even on a local server and database configuration. This is a known issue that has been tracked as DDTS number CSCin66495.

The solution is to add an entry for the server IP address to the /.rhosts file.

J.2.20 Using the get nestate Command

The **get nestate** command-line interface (CLI) command available in the ctm utility in the EMS server bin directory returns the provisioned operational state (NE_Info_Table: NEState) and the read-only modifiers to the operational state (NE_Info_Table: NEDiscoveryState). The **get nestate** command returns the following possible values:

- Preprovisioned
- In Service
- Out of Service
- Under Maintenance
- In Service–Initializing
- In Service–Sync Configuration

In addition, the **show nelist** command lists all of the NEs with the following information:

- NE database ID
- NE IP address
- Model type
- SID
- Network partition ID
- Operational state

J.3 Client Connectivity Problems

The CTM client might not be able to connect to the CTM server for various reasons. Complete the following procedures in the order listed until the problem is resolved.

J.3.1 Database Is Not Available

If the CTM client cannot connect to the CTM server, verify that the database is available.

Step 1 Log into the CTM server as the Oracle user.

Step 2 Enter the following command to connect to the database:

```
sqlplus ctmanager/ctm123!
```

Step 3 If the error message “maximum processes exceeded” is received, the maximum number of database connections has been reached. Close several clients or ask the database administrator to increase the maximum number of processes for the database.

J.3.2 Database Timeout Occurs

Step 1 Reduce the scope of the query by selecting a group or an NE and not the entire domain before opening tables such as the Alarm Browser, Alarm Log, Audit Log, and PM tables.

Step 2 Increase the client database query timeout period by editing the ems-client.cfg file in the C:\Cisco\TransportManagerClient\config or /opt/CiscoTransportManagerClient/config directory.

Step 3 Add hardware resources to the Oracle database server.

Step 4 Ping the Oracle database server from the client to verify the response time. Increase the bandwidth if the round-trip response time is inadequate.

J.3.3 Are the CTM Client and the CTM Server Connected?

If the database is available, check connectivity between the client and the server.

Step 1 To see the CTM server IP address, enter the following command on the Solaris workstation that is running the CTM server:

```
ifconfig -a
```

The command output looks similar to the following example:

```
hme0:flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>mtu 1500
inet 192.168.120.93 netmask ffffff00 broadcast 192.168.120.255
```

The IP address is the address following the inet field.

Step 2 To verify that the physical connection between the CTM client and the CTM server does not have problems, enter the following command from the CTM client:

```
ping <IP_address>
```

where the IP address belongs to the Solaris workstation that runs the CTM server.

Step 3 If the ping command is not successful, fix the physical connectivity; then, log into the CTM client.

J.3.4 Cannot Log In as Provisioner or Operator

Step 1 Use the default username and password to log into the CTM client:

Username: **SysAdmin**

Password: **Ctm123!**

Step 2 If the SysAdmin login is successful, but the provisioner or operator login fails, verify that the provisioner or operator exists and is not disabled. In the Domain Explorer window, choose **Administration > CTM Users** to view a table of all configured CTM users.

Step 3 If the provisioner or operator is not in the CTM Users table, the user is not configured. Configure the provisioner or operator; then, log in as that user.

Step 4 If the provisioner or operator is in the CTM Users table, select the row corresponding to that user and click the **Modify User Properties** tool to bring up the Modify CTM User Properties wizard. Verify that the Login State field is set to Enabled. If the login state is disabled, enable it and log in as the provisioner or operator. The user might have been disabled after attempting to log in with an incorrect password.

Step 5 If the password is not correct, set a new password for the user and log in again.

J.3.5 Cannot Authenticate User Message Appears

If the "Cannot authenticate user" error message is received when logging into the CTM client, the CTM server might be initializing. Wait for five minutes while the CTM server finishes initializing; then, try to log in again. Alternately, check your username and password and enter them again. The username and password are case sensitive.

J.4 Client Operational Problems

This section describes troubleshooting procedures for CTM client operational problems.

J.4.1 Model Index Is Unknown

If a new NE is added to the CTM domain and marked as In Service, but the model index is unknown, complete the following steps:

Step 1 Verify that the IP address and other parameters are entered correctly.

Step 2 The CTM server might not be able to establish connectivity to the GNE for the NE. Verify that the GNE for the NE is marked as In Service, and that the GNE is correctly populated in the CTM domain.

Step 3 Verify that the GNE is DCC-connected to the NE.

Step 4 The CTM server might not recognize the NE's software version. In the Domain Explorer tree, select the NE and choose **Fault > Test NE Connectivity**. If the NE is available, contact Cisco Systems and verify that the version of the software on the NE is compatible with the CTM server being used. Use the Supported NE Table to provide the new NE software version that the CTM server will recognize.

Step 5 The CTM server might be configured to attempt communication with new NEs after a certain delay. To change the health poll frequency:

a. In the Domain Explorer window, choose **Administration > Control Panel** and click **NE Service**.

b. In the NE Poller tab, look at the NE Health Poll Interval field. The default is 240 seconds. If the value is too large, there might be a communication delay between CTM and the NEs. Under normal conditions, the CTM server attempts communication with new NEs for no more than twice the number of seconds specified in the NE Health Poll Interval field.

J.4.2 Cannot Delete an NE

If an NE cannot be deleted, verify that the user logged in as SuperUser or NetworkAdmin—not as a Provisioner or Operator. Provisioners and Operators cannot delete NEs. If the user logged in as Provisioner or Operator, restart the CTM client session and log in as SuperUser.

J.4.3 CTC Fails to Start

If CTC cannot be started for a CTC-based NE, complete the following steps:

Step 1 If an error occurs while opening the NE Explorer yet the CTC progress screen and login dialog boxes appear, the CTC username or password might be incorrect.

a. Choose **Administration > CTM Users**.

b. In the CTM Users table, choose **Edit > Modify**. The Modify CTM User Properties wizard opens.

c. Click **Next** to move to the CTC/Craft User Properties panel and change the CTC username and password to match those configured on the device. Click **Finish**.

Step 2 If the CTC progress screen idles for a long time before the login dialog box appears, there might be problems with network connectivity to the device.

a. From a DOS command window or a Sun Solaris terminal, ping the device.

b. If no response is received, set up routes so that the device is available; then, restart CTC. If CTC does not start, the workstation might have resource constraints.

c. Close some open applications and try again.

d. Close some instances of CTC that are managing another group of CTC-based NEs and try again.

Step 3 If the GNE for the selected NE was not found, there might be a mismatch between the GNE specified for the device and the available GNEs. This means that the data in the database is corrupt. Contact Cisco technical support for assistance.

J.4.4 Added a New Software Version to the Wrong NE

Step 1 In the Domain Explorer window, choose **Administration > Supported NE Table**.

Step 2 In the Supported NE Table, select the incorrect entry and choose **Edit > Delete**.

Step 3 Click **OK** in the confirmation dialog box.

Step 4 Select the correct NE row from the Supported NE Table.

Step 5 Add the correct software version.

Step 6 In the Domain Explorer > Network Element Properties pane, set the operational state of all NEs that are behaving erroneously to **Out of Service**.

Step 7 Click **Save**.

Step 8 In the Network Element Properties pane, set the operational state of all the NEs back to **In Service**.

Step 9 Click **Save**.

J.4.5 Cannot Delete a Subnetwork

If a subnetwork cannot be deleted from the Subnetwork Explorer, complete the following steps:

Step 1 Verify that the user logged in as a SuperUser—not as a Provisioner or an Operator. Provisioners and Operators cannot delete subnetworks. If the user logged in as a Provisioner or Operator, restart the CTM client session and log in as a SuperUser.

Step 2 Verify that the target subnetwork does not contain NEs. Move all NEs to another subnetwork before deleting the empty target subnetwork.

J.4.6 Cannot Move an NE Between Subnetworks

When automatic grouping of NEs in subnetworks is enabled, you cannot move NEs between subnetworks. To move NEs from one subnetwork to another:

Step 1 In the Domain Explorer window, choose **Administration > Control Panel.**

Step 2 In the Control Panel, click **UI Properties**.

Step 3 Under Subnetwork Grouping, uncheck the **Automatically Group NEs in Subnetworks** check box.

Step 4 Click **Save**.

J.4.7 Cannot Schedule Jobs

The CTM client can schedule three types of administrative tasks:

- Software download
- Memory backup
- Memory restore

CTM maintains an Error Log and Audit Log to track potential problems. To view the Error Log or Audit Log:

Step 1 In the Domain Explorer window, choose **Administration > Audit Log** or **Error Log**.

Step 2 Look for errors related to software download, memory backup, or memory restore.

J.4.8 ONS 15800, ONS 15801, or ONS 15808 NE Generates Too Many Alarms

Occasionally, ONS 15800, ONS 15801, and ONS 15808 NEs generate so many alarms that the CTM client cannot process all of them. Set the operational state of the NE to **Under Maintenance** while debugging the cause of the alarms:

Step 1 In the CTM Domain Explorer window, right-click the ONS 15800, ONS 15801, or ONS 15808 that is generating the large number of alarms and choose **Mark Under Maintenance**.

Step 2 Debug the ONS 15800, ONS 15801, or ONS 15808 NE to see which card is in error. Find the card that is generating the alarms and mark it as **Under Maintenance**.

Step 3 While the card is under maintenance for debugging, set the ONS 15800, ONS 15801, or ONS 15808 NE back to **In Service**.

J.4.9 Bandwidth-Intensive Operations Are Blocked

Bottlenecks in the DCN affect bandwidth-intensive operations, such as software download. Tune the timeout and retry values to match DCN performance. Log into the NE and enter the following commands:

- **ip tftp min-timeout**—Sets the minimum wait time, in seconds, before retrying the read/write request.
- **ip tftp max-timeout—**Sets the maximum wait time, in seconds, before retrying the read/write request.
- **ip tftp backoff-delay**—Sets the number of seconds to extend wait time if the read/write request times out.
- **ip tftp write-retries**—Sets the maximum number of times to retry the TFTP read/write request before declaring a failure.

J.4.10 NE Displays Incorrect Configuration Management Data

Step 1 In the Domain Explorer window, choose **Administration > Service Monitor** and verify that the NE Service is running. If it is not running, start the NE Service.

Step 2 Test NE connectivity.

a. In the Domain Explorer tree, select the NE and choose **Fault > Test NE Connectivity**. The message "*<NE_name>* (*<IP_address>*) is available" should be generated.

b. If the NE is unavailable, establish connectivity to the NE before retrieving configuration data.

J.4.11 Cannot Customize the Network Map

If an image file is not displayed while changing the Network Map background or while changing a node icon, complete the following steps:

Step 1 Choose another image file. The file might be corrupt.

Step 2 Check the size of the image file. The image file might be larger than 100 KB, which is too big to load. If the file is too big, use a smaller image file.

Step 3 Verify that the image file exists in the \images\mapbkgnds\shapefiles directory or the \images\mapicons directory. If the file is missing, it has been deleted. Reinstall the CTM client.

Note The client is bundled primarily with shape files (*.shp) and only a few map background GIF files.

J.4.12 How Do I Change Color Settings when the CTM Client Runs on a Sun Ultra 5 Workstation?

To run the client on a Sun Ultra 5 workstation, the color map must be changed from 8 bit to 24 bit. If the colors do not look right, change the color map from 8 bit (the default) to 24 bit as follows:

Step 1 To see the current color settings, enter the following command:

```
/usr/sbin/m64config -prconf
```

Command output looks similar to the following example:

```
--- Hardware Configuration for /dev/fbs/m640 ---
ASIC: version 0x7c004750
DAC: version 0x0
PROM: version 104
Card possible resolutions: 720x400x88, 640x480x60, 640x480x72, 640x480x75, 800x600x56,
800x600x60, 800x600x72, 800x600x75, 1024x768x87, 1024x768x60, 1024x768x70, 1024x768x75,
1280x1024x75, 1280x1024x60, 1152x900x66, 1152x900x76, 1280x1024x67, 1280x800x76,
1280x1024x85
1280x1024x76, 1152x864x75, 1024x768x77, 1024x800x84, vga, svga, 1152, 1280, 800x600,
1024x768, 1280x1024, 1152x900
Monitor possible resolutions: 720x400x70, 720x400x88, 640x480x60, 640x480x67, 640x480x72,
640x480x75, 800x600x56, 800x600x60, 800x600x72, 800x600x75, 832x624x75, 1024x768x60,
1024x768x70, 1024x768x75, 1280x1024x75, 1152x870x75, 1152x900x66, 1152x900x76,
1280x1024x67, 1280x1024x76, vga, svga, 1152, 1280, 800x600, 1024x768, 1280x1024, 1152x900
Possible depths: 8, 24
Current resolution setting: 1280x1024x76
Current depth: 8
```

Step 2 To change the color setting to 24 bit, log in as the root user and enter the following commands:

```
su
Password: <password>
/usr/sbin/m64config -depth 24 -res 1152x900x76
```

Step 3 Reboot the workstation for the new color settings to take effect.

Note The resolution in 24-bit depth is a little lower than is possible with 8-bit depth (1152 x 900 x 76 versus 1280 x 1024 x 76), but the difference is hardly noticeable.

J.4.13 How Do I Collect Thread Dumps?

Thread dumps are helpful references when debugging the CTM process. To collect thread dumps:

Step 1 Log into the server workstation as the root user.

Step 2 On the command line, enter the following command:

thread_dumper [\<*Group/Service*>\]

where:

- *Group* is the group name for which to collect thread dumps. It can be:
  - SM
  - SNMPTRAP
  - NE
  - PM
  - GW
- *Service* is the service name for which the thread dump is required. It can be:
  - SMService
  - SNMPTrapService
  - CORBAGWService
  - ONS15216NEService
  - ONS15302NEService
  - ONS15305NEService
  - ONS15310NEService
  - ONS15327NEService
  - ONS15454NEService
  - ONS15454SDHNEService
  - ONS15501NEService
  - ONS15530NEService
  - ONS15540NEService
  - ONS15600NEService
  - ONS15600SDHNEService
  - ONS15800NEService
  - ONS15801NEService

- ONS15808NEService
- UnmanagedNEService
- ONS15216PMService
- ONS15302PMService
- ONS15305PMService
- ONS15310PMService
- ONS15327PMService
- ONS15454PMService
- ONS15454SDHPMService
- ONS15501PMService
- ONS15530PMService
- ONS15540PMService
- ONS15600PMService
- ONS15600SDHPMService
- ONS15800PMService
- ONS15801PMService
- ONS15808PMService

J.4.14 How Do I Enable or Disable the Automatic Refresh Data Action?

The automatic Refresh Data feature automatically refreshes all data being displayed by CTM. When automatic refresh is enabled, you receive the following prompt:

```
Refresh Data action suggested. This action will result in closing all windows and might
take some time. Do you want to continue? {Yes | No}
```

In an unstable environment where NEs are synchronizing or NEs change their operational state frequently, you might receive the preceding prompt continuously. To disable the prompt:

Step 1 In the Domain Explorer window, choose **Edit > User Preferences**. The User Preferences dialog box opens.

Step 2 Click the **Miscellaneous** tab.

Step 3 To disable the prompt, uncheck the **Enable Refresh Data Timer** check box. (To enable the prompt, leave the check box checked.)

Step 4 Click **OK**.

J.4.15 How Do I Replace the Alarm Interface Panel?

The Alarm Interface Panel (AIP) provides surge protection for CTC-based NEs. This panel has a nonvolatile memory chip that stores the unique node address known as the MAC address. The MAC address identifies the nodes that support circuits. It allows CTM to determine circuit sources, destinations, and spans.

If an AIP fails, an alarm will be generated and the LCD display on the fan-try assemblies of the NEs will go blank. To perform an in-service replacement of the AIP, you must contact Cisco technical support. For contact information, go to the technical support website at http://www.cisco.com/tac.

You can replace the AIP on an in-service system without affecting traffic by using the circuit repair feature. See 7.2.10 Repairing a Circuit, page 7-66.

J.5 Client Debug Messages

On Windows, you can start the CTM client with a console window that displays exceptions and client debug messages. You can use these messages to help troubleshoot any client problems.

Step 1 Depending on your network size, enter one of the following commands to start the client with a console window:

```
/bin/ctm-small-debug.exe
/bin/ctm-medium-debug.exe
/bin/ctm-large-debug.exe
/bin/ctm-highend-debug.exe
```

Step 2 When the CTM client exits, the console window closes. If you want to capture and save the messages when the client exits, you must redirect the output to a file. In this case, the console will not be displayed. To save exceptions to a file, open one of the following files that corresponds to your network size:

- /bin/ctm-small-debug.lax
- /bin/ctm-medium-debug.lax
- /bin/ctm-large-debug.lax
- /bin/ctm-highend-debug.lax

Note It is strongly recommended that you save a copy of the original .lax file before modifying it.

Step 3 Using a text editor, open the appropriate .lax file and change the following lines by replacing “console” with a filename:

```
lax.stderr.redirect=console
lax.stdout.redirect=console
```

When specifying filenames, make sure to use escaped backslashes (such as c:\\myfolder\\client.log). For example, to save messages to the C:\myfolder\client.log file, change the lines to read:

```
lax.stderr.redirect=c:\\myfolder\\client.log
lax.stdout.redirect=c:\\myfolder\\client.log
```

Step 4 After modifying the .lax file, enter one of the following commands to launch the CTM client:

```
/bin/ctm-small-debug.exe
/bin/ctm-medium-debug.exe
```

```
/bin/ctm-large-debug.exe
/bin/ctm-highend-debug.exe
```

On Solaris, you can start the CTM client with a console window that displays exceptions and client debug messages. You can use these messages to help troubleshoot any client problems.

Depending on your network size, enter one of the following commands to start the client with a console window:

```
ctmcdebug-start -small
ctmcdebug-start -medium
ctmcdebug-start -large
ctmcdebug-start -highend
```

J.6 CTM GateWay/TL1 Problems

If the OSS cannot connect to CTM GateWay/TL1, or if the OSS does not receive a response, check the cables, address bindings, and configuration.

Step 1 If the connection times out, check the cables and connections.

Step 2 Verify that the address bindings between the OSS and the Solaris workstation running the CTM GateWay/TL1 service are correct.

Step 3 Using the **ping** command, verify connectivity between the OSS and the Solaris workstation running the CTM GateWay/TL1 service.

Step 4 Verify that the TCP/IP socket connection is still open for the OSS-to-CTM GateWay/TL1 port.

Step 5 Choose **Administration > Control Panel**. Click **GateWay/TL1 Service** and confirm that the service status is Active.

Step 6 Verify that the username and password under **Control Panel > Security Properties** match the user configuration of the NEs that CTM GateWay/TL1 will manage.

Step 7 Verify that the username and password in the **Domain Explorer > Network Element Properties > NE Authentication** tab match the user configuration of the NEs that CTM GateWay/TL1 will manage.

J.7 CTM GateWay/CORBA Problems

If the CTM server is installed without the CTM GateWay/CORBA option, and the CTM GateWay/CORBA option is installed later, the Control Panel does not refresh automatically after the CORBA installation to show that CTM GateWay/CORBA is installed.

This problem occurs because the CTM GateWay/CORBA installation is handled by a script that notifies the database that the component is installed, but does not notify the CTM server.

To work around this problem, click the **Refresh Data** button in the Control Panel. It might take some time for the Control Panel to show that CTM GateWay/CORBA is installed. You might need to close and reopen the Control Panel to see the change.

J.8 Cisco CRS-1 and Catalyst 6509 Problems

This section describes troubleshooting procedures for problems related to the Cisco CRS-1 and the Catalyst 6509.

J.8.1 CRS-1 Communication State Remains Unavailable After Marking the Device as In Service

Step 1 Verify that the CRS-1 is configured with "hfrems" as the username and "hfrems" as the password with "root-system" privileges. By default, CTM expects "hfrems" as both the username and password. You can change the username and password in the **Control Panel > Security Properties > CRS-1** tab.

Step 2 Enter the following commands to verify that the XML CORBA agent service is running:

```
Router(config)# xml agent corba [ssl]
Router(config)# commit
```

Note SSL is optional and enables SSL CORBA services.

Step 3 If SSL CORBA services are running, enter the following commands to verify that HTTP over SSL is running:

```
Router(config)# http server ssl
Router(config)# commit
```

Step 4 The CORBA agent on the router accepts connectivity only when the connection is done through hostname. Verify that the device IP address has an entry in DNS. If not, add an entry to the /etc/hosts file.

Step 5 Verify that CTM supports the software image that is running on the router. In the Domain Explorer, choose **Administration > Supported NE Table** and verify that the software version is supported.

Step 6 When the CRS-1 is added to CTM, the NE type is retrieved from the NE to verify that the NE is a CRS-1. If the device does not report CRS-1 as the NE type, CTM reports a loss of communication (LOC) to the NE and raises an NE type mismatch alarm.

Step 7 Verify that the NE hostname specified in DNS or in the CTM server's /etc/hosts file matches the hostname configured on the NE. If the hostnames do not match, CTM reports an LOC to the NE.

J.8.2 Catalyst 6509 Communication State Remains Unavailable After Marking the Device as In Service

Step 1 Verify that the IP address entered in CTM is configured on the Catalyst 6509. Enter the following command to configure the IP address:

```
cat6509 (enable)# set interface <logical_interface_name_like_sc0/sc1>
<IP_address_of_the_Catalyst_6509> <mask>
```

Step 2 Enter the following command to verify that the device is configured correctly with the default route:

```
cat6509 (enable)# set ip route default <gateway_IP_address>
```

Step 3 Verify that CTM supports the software image that is running on the Catalyst 6509. In the Domain Explorer, choose **Administration > Supported NE Table** and verify that the software version is supported.

Note For the Catalyst 6509, the supported software version is Release 6.3(7) or later.

Step 4 Verify that the community string shown in the Domain Explorer > Address tab is same as the community string on the device. If there is a mismatch, enter the following command to change the SNMP community string on the device:

```
cat6509 (enable)# set snmp community read-only <community_string>
```

For example:

```
cat6509 (enable)# set snmp community read-only public
```

J.8.3 CTM Does Not Receive Configuration Changed Notifications from the CRS-1

Step 1 Enter the following commands to verify that the CTM server hostname and "logging-events-level" are configured in the running configuration:

```
Router# sh run | include domain ipv4 host
Router# sh run | include logging events level informational
```

Step 2 If the CTM server hostname and "logging-events-level" are not configured in the running configuration, enter the following commands:

```
Router# conf t
Router(config)# domain ipv4 host <CTM_server_hostname> <IP_address>
Router(config)# logging events level informational
Router(config)# commit
```

J.8.4 CTM Does Not Receive Traps from the Catalyst 6509

Step 1 Enter the following command to configure the CTM server as the trap receiver on the Catalyst 6509:

```
cat6509 (enable)# set snmp trap <CTM_server_IP_address> <community_string>
```

Step 2 Enter the following command to configure the Catalyst 6509 to enable only specific traps:

```
cat6509 (enable)# set snmp trap enable <specific_trap>
```

where <*specific_trap*> is auth, bridge, chassis, config, entity, ippermit, module, stpx, syslog, systemp, vmps, or vtp.

Step 3 Enter the following command to configure the Catalyst 6509 to enable all traps:

```
cat6509 (enable)# set snmp trap enable all
```

Note The **set snmp trap enable all** command enables traps only on physical ports. For logical ports such as sc0 or sc1, you must enable traps separately. Go to Step 4.

Step 4 Enter the following command to enable traps on logical ports:

```
cat6509 (enable)# set interface trap <logical_port_name> enable
```

For example, to enable traps on the logical interface sc0, enter:

```
cat6509 (enable)# set interface trap sc0 enable
```

J.8.5 CTM Does Not Receive syslog Events from the Catalyst 6509

The Catalyst 6509 sends syslog traps only if the trap severity is both:

- Less than or equal to facility severity (which is set with the **set logging level** command)
- Less than or equal to history severity (which is set with the **set logging history severity** command)

It is recommended that you set the history severity to debugging (7).

The **show logging** command shows both the history severity and the severity for all facilities. For example, in the following output, the history severity is 7 and facility severity is 5. Syslog events of severity *X* will be triggered from the device if *X* is less than or equal to 5 and less than or equal to 7.

```
Cat6509 (enable)# show logging

Trace logging:                  disabled
Logging buffer size:            500
        timestamp option:       enabled
Logging history:
        size:                   1
        severity:               debugging(7)
Logging console:                enabled
Logging telnet:                 enabled
Logging server:                 enabled
{10.77.56.151, 172.19.75.86}
        server facility:        SYSLOG
        server severity:        debugging(7)
Current Logging Session:        enabled
Callhome Functionality:         disabled
Callhome Severity:              LOG_CRIT(2)

SMTP servers are not configured for callhome messages.

Destination addresses are not configured for callhome messages.

From Address is not configured for callhome messages.
Reply-To Address is not configured for callhome messages.


Facility            Default Severity         Current Session Severity
-------------       ----------------------   ------------------------
acl                 5                        5
callhome            2                        2
cdp                 4                        4
cops                3                        3
...
```

```
...
sys                 5                          5
...
vmps                2                          2
vtp                 2                          2

0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
```

J.8.6 CTM Does Not Collect Historical PM Data for the CRS-1

Step 1 Verify that PM collection is enabled for the CRS-1. To do this, go to the Network Element Properties > Status tab and in the PM Collection area, check the **15 Min** check box. Click **Save**. Also, verify that the CRS-1 PM Service Status is Active in the Control Panel window.

Step 2 Enter the following commands to verify that the correct PM configuration is in the running configuration on the CRS-1:

```
Router(config)#  show run perf

performance-mgmt resources tftp-server <IP_address_of_server> directory
<directory_on_TFTP_server>
performance-mgmt statistics bgp template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics mpls ldp template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics node cpu template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics interface generic-counters template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics interface data-rates template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics mpls TE-link template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics node memory template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics node process template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics mpls TE-tunnel template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics mpls interface template default
 sample-size 1
```

```
 sample-interval 15
!
```

Step 3 If the files are not being dumped to the target directory on the TFTP server, verify that the TFTP server is using the correct tftpd (tftp daemon binary). The tftpd should be a version that allows the CRS-1 to create new files in the specified directory. The default tftpd only allows pre-existing TFTP files to be written. The default tftpd does not create new TFTP files.

Step 4 If the files appear on the TFTP server but do not appear in the PM table, verify that the CTM server is being notified of PM TFTP file dumping events. To do this, choose **Fault > Alarm Log** and check for events that arrive every 15 minutes and resemble the following output:

```
pm_collector[301]: %PM_COLLECTOR-6-TFTP_SEND : Successfully dumped
file:tftp://<IP_address><TFTP_directory><NE_name>_node_process_1100886887.212000
```

Step 5 If events do not appear after 15 minutes, verify that configuration change notifications are enabled. See J.8.3 CTM Does Not Receive Configuration Changed Notifications from the CRS-1, page J-23.

Step 6 If events are present, verify that the TFTP server is reachable from the CTM server. To do this, ping the IP address that is present in the event notification. If the IP address is not reachable, configure the routes so that it becomes reachable. Alternately, include a mapping file in the /opt/CiscoTransportManagerServer/cfg/hfr/IPAddressMapping.cfg directory that includes the following mapping:

```
<IP_address_in_event_notification> <reachable_IP_address_of_the_same_TFTP_server>
```

For example:

```
172.19.64.51 223.255.254.254
```

J.8.7 CRS-1 PM Tables Collect Data at the Wrong Collection Interval

You might experience a problem where the PM data collection interval is set to 15 minutes, but the CRS-1 PM tables are collecting data more frequently (or less frequently).

The CRS-1 collects and dumps data to a binary file on a TFTP server at user-configured intervals based on the IOS-XR CLI. After dumping the PM data, the CRS-1 notifies CTM with the location of the file. CTM then collects PM data from the CRS-1. Therefore, you should configure the CRS-1 to collect data every 15 minutes.

J.8.8 Memory Backup or Restore Fails for the CRS-1

Step 1 Verify that the NE is in service and the communication state is Available.

Step 2 Verify that you can ping the CTM server from the NE. The NE is used as a TFTP client for downloading the configuration file.

Step 3 In the /etc/inetd.conf file, verify that the TFTP server is enabled on the CTM server. Also, verify that the specified tftpboot directory has the correct permissions.

J.8.9 How Do I Back Up the CRS-1 Configuration File Automatically Whenever the Configuration Is Changed on the Router?

Step 1 In the Domain Explorer, choose **Administration > Control Panel**.

Step 2 Click **NE Service**.

Step 3 In the NE AutoBackup tab, choose **Cisco CRS-1** as the NE model. Alternately, choose **All NE Models**.

Step 4 Check the **Enable Auto Backup** check box.

Step 5 Specify the number of backup copies and the backup time.

Step 6 Click **Save**.

J.8.10 For the CRS-1, CTM Does Not Automatically Discover Neighboring NEs

Step 1 Verify that there is a physical link between the two NEs.

Step 2 Complete one of the following options, depending on your configuration:

- If the link is an Ethernet link, bring up the interfaces on both NEs. For example, enter the following commands on the first router:

```
Router-1(config)# int GigabitEthernet0/2/0/0
Router-1(config-if) ipv4 address <IP_address> <mask>
Router-1(config-if) no shutdown
Router-1(config-if) commit
```

  Enter the following commands on the second router:

```
Router-2(config)# int GigabitEthernet0/1/0/0
Router-2(config-if) ipv4 address <IP_address> <mask>
Router-2(config-if) no shutdown
Router-2(config-if) commit
```

- If the link is a POS link, enter the following commands on the first router:

```
Router-1(config)# int POS 0/2/0/0
Router-1(config-if) ipv4 address <IP_address> <mask>
Router-1(config-if) no shutdown
Router-1(config-if) commit
```

  Enter the following commands on the second router:

```
Router-2(config)# int POS 0/1/0/0
Router-2(config-if) ipv4 address <IP_address> <mask>
Router-2(config-if) no shutdown
Router-2(config-if) commit
```

  Verify that the SONET controllers are up. For example, enter the following commands:

```
Router-1(config)# controller SONET 0/2/0/0
Router-1(config-sonet)# no shutdown
Router-1(config-sonet)# commit

Router-2(config)# controller SONET 0/1/0/0
Router-2(config-sonet)# no shutdown
Router-2(config-sonet)# commit
```

Step 3 Enter the following commands to enable CDP on both NEs:

```
Router-1(config)# cdp
Router-1(config)# commit

Router-2(config)# cdp
Router-2(config)# commit
```

J.8.11 Cannot Delete an Out-of-Service NE from CTM

If you cannot delete an out-of-service NE from CTM, follow the procedure in 3.5.7.3 Using the prune_ne.sh Script to Remove an Out-of-Service NE from the Database, page 3-27.

J.8.12 Software Version Is Not Reported in the Domain Explorer and the NE Software Table Is Empty

If you cannot see the software version in the Domain Explorer > Identification tab and NE Software table is empty, complete the following steps:

Step 1 Verify that the NE is in service and the communication state is Available.

Step 2 Verify that the device is configured with either Telnet or SSH.

J.8.13 Cannot Use Configuration > Telnet/SSH from the CRS-1 NE Explorer

If you cannot use Configuration > Telnet/SSH from the CRS-1 NE Explorer, try pinging the NE from the CTM client. You might be able to reach the NE from the CTM server but not from the client if they are in different subnets.

J.8.14 How Do I Configure Telnet on the CRS-1?

To configure Telnet on the CRS-1, log into the router through the console and enter the following commands:

```
Router# conf t
Router(config)# telnet ipv4 server
Router(config)# commit
```

J.8.15 How Do I Configure SSH on the CRS-1?

Step 1 Enter the following command to verify that the security PIE(k9) is installed and activate on the router. The PIE(k9) is required for encryption, decryption, IPSec, SSH, SSL, and PKI:

```
Router# sh install active
```

Step 2 Enter the following command to verify that DSA keys have been generated on the router:

```
Router# crypto key generate dsa
```

Step 3 Enter the following command to verify that RSA keys have been generated on the router:

```
Router# crypto key generate rsa
```

Step 4 Enter the following command to verify that SSH is enabled on the router:

```
Router# crypto key generate rsa
```

Step 5 Enter the following command to enable the SSH server on the router:

```
Router(config)# ssh server enable
```

J.8.16 How Do I Create and Grant Certificates for SSL-Configured CRS-1 NEs?

See 5.4.25 Configuring Secure Socket Layer for the CRS-1 and XR 12000, page 5-188.

J.8.17 How Do I Trigger a linkDown or linkUp Trap from the Catalyst 6509?

Complete one of the following options:

- To trigger a linkDown trap from the Catalyst 6509, enter the following command:

  ```
  cat6509 (enable)# set port disable <module_number/port_number>
  ```

  For example:

  ```
  cat6509 (enable)# set port disable 5/1
  ```

- To trigger a linkUp trap from the Catalyst 6509, enter the following command:

  ```
  cat6509 (enable)# set port enable <module_number/port_number>
  ```

  For example:

  ```
  cat6509 (enable)# set port enable 5/1
  ```

J.8.18 How Do I View the SNMP Configuration on the Catalyst 6509?

To view the SNMP configuration on the Catalyst 6509, enter the following command:

```
cat6509 (enable)# show snmp
```

J.8.19 How Do I Load a Software Image on the Catalyst 6509?

Complete the following steps:

Step 1 Enter the following command to view all the software images on the Catalyst 6509:

```
cat6509 (enable)# dir bootflash:
```

The output is similar to the following example:

```
-#- -length- -----date/time------ name
2  5849256 Aug 09 2004 14:41:25 cat6000-sup2.6-3-7.bin
3  8801412 Aug 09 2004 15:30:57 cat6000-sup2k8.8-3-2.bin
4  5713736 Aug 11 2004 13:08:02 cat6000-sup2.6-3-2a.bin
5  8182352 Aug 12 2004 09:15:00 cat6000-sup2k8.8-2-1.bin
17     1786 Aug 23 2004 14:16:30 6509svt-171-180
19     1688 Sep 24 2004 15:26:40 6509svt-171-180.cfg

3346628 bytes available (28634940 bytes used)
```

Step 2 Enter the following command to retrieve the image name that is currently on the device:

```
cat6509 (enable)# whichboot
```

The output is similar to the following example:

```
Boot image name is 'bootflash:cat6000-sup2.6-3-7.bin'.
```

Step 3 Enter the following command to delete the existing image:

```
cat6509 (enable)# del <image_name>
```

Step 4 Enter the following command to remove the deleted image:

```
cat6509 (enable)# squeeze bootflash:
```

Step 5 Enter the following commands to copy the image to flash memory:

```
cat6509 (enable)# copy tftp flash
IP address or name of remotehost[]? <TFTP_server_IP_address>
Name of file to copy from []? <Full_path_name_and_filename_of_the_image_location>
```

For example:

```
tftpboot/cat6k/7-2/<image_name>
```

Step 6 Enter the following command to verify that the downloaded image exists on the device:

```
cat6509 (enable)# dir bootflash:
```

Step 7 Enter the following command to verify that the download was successful:

```
cat6509 (enable)# verify <image_name>
```

Step 8 Enter the following command to clear the flash system:

```
cat6509 (enable)# clear boot system flash bootflash:<previous_image_name>
```

Step 9 Enter the following command to set the boot system flash with the new image name:

```
cat6509 (enable)# set boot system flash bootflash:<new_image_name> prepend
```

Step 10 Enter the following command to reset the device:

```
cat6509 (enable)# reset
```

J.9 XR 12000 Problems

This section describes troubleshooting procedures for problems related to the XR 12000.

J.9.1 Reporting XR 12000 Issues

When reporting an XR 12000 problem, include detailed steps to reproduce the problem and the software version(s) of the NE(s) to which the problem applies. Also, enter the following router CLI commands on the XR 12000 and collect the data:

```
show version
show platform
show inventory
show ipv4 interface brief
show running-config
show events
show log events buffer all-in-buffer
```

Turn on trace level debugging in the Control Panel for the service in question, wait until the problem occurs, and collect the GSRIOXNEService logs from /opt/CiscoTransportManagerServer/log.

J.9.2 CTM Cannot Discover an XR 12000 Node

Complete the following steps if CTM cannot discover an XR 12000 node:

Step 1 Verify that the NE is configured with “hfrems” as the username and “hfrems” as the password with “root-system” privileges. By default, CTM expects the username and password to be hfrems/hfrems. You can change the security properties from the Control Panel > Security Properties pane > XR 12000 tab. CTM will use the new username and password to authenticate all XR 12000 devices in the domain.

Step 2 Check whether the XML CORBA agent service is running. To configure the XML CORBA agent, enter:

```
Router(config)# xml agent corba [ssl]
Router(config)# commit
```

Note ssl is optional and enables SSL CORBA services.

If SSL CORBA services are activated, enter the following commands to check whether HTTP over SSL is running:

```
Router(config)# http server ssl
Router(config)# commit
```

Step 3 The CORBA agent on the router accepts connections only when using the hostname. Check to see if the device IP address has an entry in DNS. If DNS is not used, add an entry in the /etc/hosts file.

Step 4 Verify that CTM supports the software version that is running on the router. The CTM release notes list the CTM-supported NE software versions. Go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/optnet/ctm/ctmreln/index.htm.

Step 5 When an NE is added to CTM, the NE type is retrieved to verify whether the NE is an XR 12000. If the device is not of NE type XR 12000, the NE is moved to an LOC state in CTM and an NE type mismatch alarm is raised.

Step 6 The NE hostname specified in DNS or in the CTM server /etc/hosts file must match the hostname configured on the NE. If the hostnames do not match, the NE is moved to an LOC state in CTM.

J.9.3 XR 12000 Status Is Not Immediately Reflected in the Domain Explorer

If the LAN cable is removed, there is a delay before the status of the XR 12000 is updated in the Domain Explorer. It might take several minutes or more to reflect the status as unreachable if the router is disconnected.

If you want the status to be updated sooner, you must modify the jacorb.connection.client.pending_reply_timeout parameter in the /opt/CiscoTransportManagerServer/openfusion/classes/jacorb.properties file. The default timeout is 5 minutes (300000 ms). Updates take approximately the health poll interval plus two times the jacorb.connection.client.pending_reply_timeout value.

J.9.4 XR 12000 Alarm and Event Reporting Issues

If CTM does not receive XR 12000 alarm and event notifications, complete the following steps:

Step 1 Enter the following commands to verify that the CTM server hostname and "logging-events-level" are configured in the running configuration:

```
Router# sh run | include domain ipv4 host
Router# sh run | include logging events level informational
```

Step 2 If the CTM server hostname and "logging-events-level" are not configured in the running configuration, enter the following commands:

```
Router# conf t
Router(config)# domain ipv4 host <CTM_server_hostname> <IP_address>
Router(config)# logging events level informational
Router(config)# commit
```

J.9.5 XR 12000 PM Collection Issues

The XR 12000 collects and dumps data to a binary file on a TFTP server at intervals configured by the user through the CLI. After dumping the performance data, the XR 12000 sends a notification indicating the location of the file. Upon receiving this notification, CTM collects performance data from the XR 12000. Therefore, the network operator should configure the XR 12000 to collect data every 15 minutes.

Step 1 Enter the following command to verify whether the TFTP server and directory are configured in the running configuration:

```
performance-mgmt resources tftp-server <server_IP_address> directory
<directory_on_TFTP_server>
```

Step 2 Enter the following commands to verify that the router's running configuration contains the correct PM configuration:

```
performance-mgmt statistics bgp template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics mpls ldp template default
 sample-size 1
 sample-interval 15
!
performance-mgmt statistics node cpu template default
 sample-size 1
 sample-interval 15
!
.
.
.
.
```

Step 3 After dumping the performance data, the XR 12000 sends a notification indicating the location of the file. This notification is logged in the Alarm Log every 15 minutes and triggers the CTM server connecting to the TFTP server. Check for notifications in the Alarm Log that look similar to the following:

```
pm_collector[301]: %PM_COLLECTOR-6-TFTP_SEND : Successfully dumped
file:tftp://<IP_address><TFTP_directory><NE_name>_node_process_1100886887.212000
```

J.9.6 XR 12000 BGP and CDP Neighbor Discovery Issues

CTM discovers all the CDP and BGP neighbor routers and adds them to the tree view if the CDP or BGP is enabled on the router. CDP and BGP neighbor discovery occurs after the NE is synchronized. If the neighbors are not discovered, enter the following CLI commands to check whether CDP or BGP is enabled on the router and interfaces:

```
show bgp neighbors
show cdp neighbors
```

J.9.7 XR 12000 NE Explorer Applications Are Disabled

The CTM NE Explorer enables only those applications for which the XML version matches on CTM and the router. If an NE Explorer application is disabled, there might be a version mismatch. Do the following:

- Collect all the XML files from the <*CTM_home*>/cfg/metadata directory.
- Run the <*CTM_home*>/bin/vwdata.sh script to collect the hfr_version_info database table entries.

On Windows, if an NE Explorer or GUI application returns an error, repeat the same operation after invoking the GUI by entering one of the following commands, depending on your network size:

```
<CTM_home>/bin/ctm-small-debug.exe
<CTM_home>/bin/ctm-medium-debug.exe
<CTM_home>/bin/ctm-large-debug.exe
```

This opens a console that logs all the exceptions. Capture the console log for debugging.

On UNIX, enter the *<CTM_home>*/bin/ctmcdebug-start command to start the client and repeat the same operation. This generates the error and exception messages on the terminal. Capture the terminal messages for debugging.

J.10 Problems with MGX Voice Gateway Devices

This section describes troubleshooting procedures for problems related to the MGX Voice Gateway devices.

J.10.1 Discovery Mechanism

CTM manages the Private Network-Network Interface (PNNI). The ILMITopoc process uses SNMP protocol to discover the physical PNNI network. All the discovered nodes are displayed in the MGX NE GUIs (Configuration Center, Diagnostics Center, Statistics Report, and Chassis View). CTM is notified of all subsequent changes in the network through traps for MGX nodes.

Once the ILMITopoc process discovers all the nodes, it sends all the nodes to the topod process. Topod then sends these nodes and trunks to other processes in CTM such as ooemc, NMServer, nts, and so on.

J.10.2 Discovery Issues at Startup

This section includes the following information:

- J.10.2.1 No Nodes Are Discovered, page J-34
- J.10.2.2 Node Name Is Incorrect in the Database, page J-35
- J.10.2.3 Node IP Is Incorrect in the Database, page J-36
- J.10.2.4 Node Alarm Is Shown Incorrectly in the Database, page J-36
- J.10.2.5 Reachable Node Is Shown as Unreachable, page J-37
- J.10.2.6 CTM State Is Incorrect, page J-37

J.10.2.1 No Nodes Are Discovered

If no nodes are in the CTM database, complete the following steps:

Step 1 Verify that the nodes are IP-reachable. Complete the following substeps:

a. Enter the following CLI commands to retrieve the primary IP address of the node:

```
dspndparms
dspipif
```

b. Enter the following command to check whether CTM has IP connectivity to the node:

```
ping <node_IP_address>
```

Step 2 If CTM has IP connectivity to the nodes, verify that the community strings of the gateway nodes are correct. Complete the following substeps:

a. Enter the following command on the switch CLI of the node that cannot be discovered:

```
dspsnmp
```

b. Compare this community string with the community string in the node_info table. The community string in the node_info table is encrypted. You will need to decrypt this string and verify it.

Step 3 For MGX nodes, if persistent topology is enabled on the switch gateway and some nodes in a peer group are not discovered, complete the following substeps:

a. Enter the following CLI command to verify that persistent topology is enabled on the gateway in the peer group:

```
dsptopogw
```

b. If the gateway flag is enabled, enter the following CLI command to verify that the node is part of the list of nodes on the gateway:

```
dsptopondlist
```

Defect information—Collect the following information for further analysis:

- Topod.log and ILMITopoc.log.
- Data in the node_info table.
- Output of dspndparms, dspsnmp, and dspipif on the MGX node.

J.10.2.2 Node Name Is Incorrect in the Database

If the node name of the standalone MGX node is incorrect, complete the following steps:

Step 1 If the node table contains the correct name, complete the following substeps:

a. Enter the following command to dump the cache of topod and ILMITopoc:

```
kill -USR1 <process>
```

b. From the data collected, verify which process contains the incorrect information. If the information is correct in all processes, open a new instance of the GUI and verify whether the problem still exists.

Step 2 If the node table contains the incorrect name, check the ILMITopoc.log file to see from which node it collected the wrong information. Complete the following substeps:

a. Enter the following command:

```
snmpget -c <community> <IP_address> 1.3.6.1.2.1.1.5
```

b. Verify that the name received as a response is correct. If the name received is incorrect, verify the name on the switch.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log and topod.log.
- Dump outputs of ILMITopoc and topod. Enter the following command:

```
kill -USR1 signal <process>
```

- Output of the switch CLI, selnd, and dbnds.

J.10.2.3 Node IP Is Incorrect in the Database

Step 1 If the node table contains the correct IP address, complete the following substeps:

a. Enter the following command to dump the cache of topod and ILMITopoc:

```
kill -USR1 <process>
```

b. From the data collected, verify which process has the incorrect information. If the information is correct in all processes, open a new instance of the GUI and verify whether the problem still exists.

Step 2 If the node table does not have the IP address set correctly, verify whether the node is managed by the LAN IP address. In CTM, since the node does not have any PNNI trunks and the persistent topology feature is not enabled, the node is managed by the LAN IP address by default.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log and topod.log.
- Dump outputs of ILMITopoc and topod. Enter the following command:

```
kill -USR1 signal <process>
```

- Collect the output of the switch CLI, selnd, and dbnds.

J.10.2.4 Node Alarm Is Shown Incorrectly in the Database

Step 1 Enter the following command to dump the cache of topod and ILMITopoc:

```
kill -USR1 <process>
```

Step 2 From the data collected, verify which process contains the incorrect information.

Step 3 If the node table does not have the node alarm status set correctly, check the ILMITopoc.log file and enter the following command:

```
snmpget -c <community string> <IP_address> 1.3.6.1.4.1.351.110.1.1.14
```

The **snmpget** command returns the alarm state of the node, where 1 = Clear, 2 = Minor, 3 = Major, and 4 = Critical.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log and topod.log.
- Dump outputs of ILMITopoc and topod. Enter the following command:

```
kill -USR1 signal <process>
```

- Collect the output of the switch CLI, selnd, and dbnds.

J.10.2.5 Reachable Node Is Shown as Unreachable

If a node that is reachable from CTM is shown as unreachable in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, complete the following steps:

Step 1 If the node table reports the alarm state of this node as minor, major, critical, or clear, complete the following substeps:

a. Enter the following command to dump the cache of NMServer, topod, and ILMITopoc:

```
kill -USR1 signal <process>
```

b. Check the data collected in the /opt/svplus/log directory and verify whether the node alarm status is correct. If the alarm status is correct in the cache dump, open a new instance of the GUI and check whether the node shows the correct alarm status in that window.

Step 2 If the node table shows the alarm state of an MGX node as unreachable, complete the following substeps:

a. Verify that the node is IP-reachable from CTM.

b. Ping the active IP address of the node. The active IP address is the IP address of the node that is populated in the node table.

c. Enter the following CLI command to retrieve the community string of the node:

```
dspsnmp
```

d. Verify that the community string in the node_info table is the same as the community string on the node.

e. Check the nts logs to see if nts has declared the node as reachable. See J.10.13.1 NTS, page J-127. If nts has declared the node as reachable, check the topod.log for "nonRoutingNodeMsg" for this node. Verify that the alarm status in this message is the correct alarm status.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log, topod.log, NMServer.*.log, nts.*.log, and ooemc*log.
- Dump outputs of ILMITopoc, topod, and NMServer. Enter the following command:

```
kill -USR1 signal <process>
```

- Output of the switch CLI, selnd, and dbnds.

J.10.2.6 CTM State Is Incorrect

If the management state of the node in the node table (mgmt_state column) shows as DOWN (2) or UNKNOWN (0) even when the node is reachable by IP, complete the following steps:

Step 1 Check the trap manager registration of the CTM station on the node. Log into the node and enter the following command to check whether the CTM station has registered to the node for traps. This is required for the node to be declared as manageable (mgmt_state = UP).

```
dsptrapmgr
```

Step 2 Enter the community strings (SNMP-GET and SNMP-SET) of the node through the Domain Explorer > Network Element Properties pane > NE Authentication tab. The SNMP strings might be incorrect in the node_info table. The strings can be verified if the decrypt tool for the encrypted strings is available in the database.

Step 3 Check the nts.log to see if trap registration succeeded for the node. See J.10.13.1 NTS, page J-127.

Step 4 Save ILMITopoc.log, topod.log, and ooemc*.log for analysis.

J.10.3 Discovery Issues at Runtime

This section includes the following information:

- J.10.3.1 Node Is Not Shown in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-38
- J.10.3.2 Node Name Change Is Not Updated in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-39
- J.10.3.3 Node IP Address Change Is Not Updated in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-39

J.10.3.1 Node Is Not Shown in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

If a dynamically added routing node is not shown in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, complete the following steps:

Step 1 If the node table has an entry for the node, complete the following substeps:

a. Enter the following command to dump the cache of NMServer, topod, and ILMITopoc:

```
kill -USR1 signal <process>
```

b. Check the data collected in the /usr/user/svplus/log directory and verify whether the node is present in the cache dumps. If the node is present, open a new instance of the GUI and check whether the node is visible in that GUI.

Step 2 If the node table does not have an entry for the node, complete the following substeps:

a. Check the ILMItopoc log and verify whether it received a 70005 and 70201 trap (if the persistent topology feature is enabled).

b. If you see the trap in the log, verify that ILMITopoc's SNMP requests issued after receiving the trap are successful. If an SNMP request does not go through, verify whether CTM has IP and SNMP connectivity to the newly added node.

c. If you do not see the traps in the ILMITopoc.log, see J.10.13.1 NTS, page J-127.

Step 3 Complete the following substeps to collect defect information for analysis:

a. Save ILMITopoc.log, topod.log, NMServer.log, and nts.*.log.

b. Enter the following command to collect the dump outputs of ILMITopoc, topod, and NMServer:

```
kill -USR1 signal <process>
```

c. Collect the output of the switch CLI, selnd, and dbnds.

Step 4 If the preceding steps do not solve the problem, delete the node from the network and add it again.

J.10.3.2 Node Name Change Is Not Updated in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

If changes to the node name are not reflected on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, complete the following steps:

Step 1 If the node table has an entry for the node with the correct name, complete the following substeps:

a. Enter the following command to dump the cache of NMServer, topod, and ILMITopoc:

```
kill -USR1 signal <process>
```

b. Check the data collected in the /usr/user/svplus/log directory and verify whether the node name is correct in the cache dumps. If the node name is correct, open a new instance of the GUI and check whether the node name is correct in that GUI.

Step 2 If the node table does not have an entry for the node with the correct name, complete the following substeps:

a. Check the ILMItopoc log and verify whether it received a 60006 and 70202 trap.

b. If you see the trap in the log, verify that ILMITopoc updates its cache based on the trap. If it fails to update the node name, ILMITopoc.log will contain the message "%ILMITopoc-3-updateFailed: <Node_c::updateName> Failed to update node name."

c. If you do not see the traps in the ILMITopoc.log, see J.10.13.1 NTS, page J-127.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log, topod.log, NMServer.log, and nts.*.log.
- Dump outputs of ILMITopoc, topod, and NMServer. Enter the following command:

```
kill -USR1 signal <process>
```

- Collect the output of the switch CLI, selnd, and dbnds.

J.10.3.3 Node IP Address Change Is Not Updated in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

If the node IP address is not updated dynamically in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, complete the following steps:

Step 1 If the node table has an entry for the node with the correct IP address, complete the following substeps:

a. Enter the following command to dump the cache of NMServer, topod, and ILMITopoc:

```
kill -USR1 signal <process>
```

b. Check the data collected in the /opt/svplus/log directory and verify whether the IP address is correct in the cache dumps. If the IP address is correct, open a new instance of the GUI and check whether the IP address is correct in that GUI.

Step 2 If the node table does not have an entry for the node with the correct IP address, complete the following substeps:

a. Check the ILMItopoc log and verify whether it received a 60007 and 70202 trap.

b. If you see the trap in the log, verify that ILMITopoc updates its cache based on the trap.

c. If you do not see the traps in the ILMITopoc.log, see J.10.13.1 NTS, page J-127.

Defect information—Collect the following information for further analysis:

- ILMITopoc.log, topod.log, NMServer.log, and nts.*.log.
- Dump outputs of ILMITopoc, topod, and NMServer. Enter the following command:

  kill -USR1 signal *<process>*

- Collect the output of the switch CLI, selnd, and dbnds.

J.10.4 Equipment Management Problems

This section describes troubleshooting procedures for equipment management problems on the Cisco MGX devices.

J.10.4.1 Equipment Management Declares Successful Node Resync when Node Mode Is 3

MGX nodes are managed by the ooemc component in CTM. Equipment management (EM) uses coldstart, warmstart, and periodic resync to synchronize network data. Each of these resync methods involves configuration file upload, parsing, and database population. The node mode in the node table indicates the state of the synchronization process. The possible node modes are 1, 2, 3, and 5. The expected mode for a successful node resync is 3. If the node mode stays in other modes for a long time, it indicates a resync problem. Any synchronization problem could be caused by the switch, SNMP, FTP, or ooemc. You must investigate different areas to identify the root cause of any synchronization problem.

The following is the flow of events in the ooemc coldstart synchronization process:

1. The topo process discovers a node in the network. The process changes the node mode in the node database table to –1. It then notifies the ooemc component for the discovery. The ooemc changes the node mode from –1 to 1 after the component begins managing the node.
2. When the nts component is able to register with the node, it sends a link up message to the ooemc that manages the node. The ooemc component changes the node mode from 1 to 2 to signify the start of the node synchronization.
3. The ooemc component sends an SNMP bulk file creation request to the switch. If the request is allowed, the switch sends a trap 60901 to CTM to signify the start of bulk file creation. When bulk file creation is complete on the switch, the switch sends a trap 60902 to CTM. After CTM receives the trap, it begins to FTP the config upload files.
4. If the upload and parsing of all config files completes without errors, the ooemc changes the node mode from 2 to 3. If the upload or parsing encounters errors for any service module on the switch, the node synchronizes partially and the ooemc changes the node mode from 2 to 4 at the end of the node synchronization process. If the error occurs on the shelf generic card file (CARD_01_CC.CF) or pnni file (PNNI_01_CC_CF), the ooemc changes the node mode from 2 to 5 to signify node sync-up failure.

J.10.4.2 Network Setup and Configuration Required for OOEMC Sync-Up Process

The EM requires network setup and CTM configuration prerequisites before it can start the sync-up process. On the switch, perform the following:

- Use the **dsptrapmgr** CLI command to verify that the CTM IP address has been added to the trap manager. If your CTM IP address is not registered with the switch, add the CTM IP address to the trap manager by entering the **addtrapmgr** <*cwm_ip*> **2500** CLI command, where 2500 is the port number and *cwm_ip* is the IP address of your CTM machine. You might need to delete other IP addresses from the trap manager list if the list is full. If the list is not full, the registration takes place automatically if CTM is configured to manage the node.
- The trap IP should have been configured on the switch properly. Whenever you configure the switch to use any IP (atm0 IP or lnPci0 IP) of the switch as primary IP, the topology component of CTM should use that IP for node discovery. You can display the primary and secondary IP information of the switch by typing the CLI command **dspndparms**. To configure the primary and secondary IP addresses, you can enter **cnfndparms** and the CLI will prompt you for options. After you have set up the primary and secondary IP addresses, you should also configure the primary IP as trap IP on the switch by entering the CLI command **cnftrapip configured_IP**, where configured_IP is the IP that you have chosen to use as the primary IP in the CLI command **cnfndparms**.
- On CTM, the following is a list of configurable parameters in the file /opt/svplus/config/emd.conf of your CTM machine that you should set up for proper problem logging:
  - "OODebug": For debugging purposes, this parameter should be set to level 6 or above; for example, the log level statement in emd.conf should be "OODebug Level 6."
  - "OOKeep": For debugging purposes, this parameter should be set to a value depending on how many log files you want to keep; for example, the statement in emd.conf should be "OOKeep 100 ooemc log files per oochild."

Note Sometimes, a different network environment requires other parameters in the same files to be tuned for correct functioning of CTM.

J.10.4.3 Node Mode Remains in 1

The node has been discovered by the network topology process in CTM, its node mode has been changed from -1 to 1 in node table entry, and it stays in mode 1 for a long period of time.

Step 1 If CTM stays in mode 1 for a long time after CTM core has been started, you need to check the trap manager on the switch. See J.10.4.2 Network Setup and Configuration Required for OOEMC Sync-Up Process, page J-41 for trap manager and trap IP setup.

Step 2 If step 1 is not an issue, then check for rtm link up message that nts sends to EMD. The ooemc will start node resync once EMD notifies the ooemc that the node is active. Therefore, the second step for debugging this mode 1 problem is to see whether rtm link up message has been received by EMD and whether it has been forwarded to the ooemc.

For example, to find the rtm link up messages received by EMD for node with ID 9, issue the following command:

```
grep RTM_LINK_UP emd* | grep "Node id 9"
```

Once the location of the rtm link up message is found in the log, view the log file for more information on notification to ooemc.

Step 3 If the rtm link up message for the node is found and the log indicates that notification to ooemc has been sent, then collect the log files and report the problem.

Step 4 If the rtm link up message cannot be found, then search for link down message. Grep RTM_LINK_DOWN from the emd log files. If the rtm link down message is found, then the node is not reachable by the nts process. Check with the network administrator and see J.10.13.1 NTS, page J-127 if RTM_LINK_UP and RTM_LINK_DOWN messages are not found.

Defect information—Collect the following information for further analysis:

- Ooemc and nts log files from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.4.4 Node Mode Remains in 2

After EMD receives the rtm link up message and the node active message has been sent to ooemc, ooemc will change the node mode from 1 to 2 and trigger the node resync process. The node resync time varies depending on the switch configuration and network activities. If the node mode stays in mode 2 for longer than the normal time for node resynchronization, there can be a problem with the node resync process.

Step 1 The debugging process for this problem is mainly focused on log file inspection. Make sure that log level of all related CTM processes is set at the right level. See J.10.4.2 Network Setup and Configuration Required for OOEMC Sync-Up Process, page J-41 for more information.

Step 2 Go to the /opt/svplus/tmp directory to check for configuration upload files.

Step 3 Determine which files have been uploaded for a node. For example, issue the following command on a node with node_id=9:

```
ls -ltr *.9
```

If files have been uploaded for this node, then the node resync process is ongoing. Make sure that the time stamps for these files refer to the current time.

Note Refer to step 6 for a list of configuration upload files.

Step 4 If there are no files uploaded for a node, it is possible that the trap IP address on the switch does not match the IP address used for node discovery. It is also possible that an SNMP request failure occurred. To check the IP addresses, perform the following:

a. Use the CLI command **dbnds** to display the IP address used for node discovery.

b. Use the CLI command **dsptrapip** to display the trap IP address.

c. If there is a mismatch, use the CLI command **cnftrapip** to reconfigure the trap IP address. Use the IP address used by CTM for node discovery. See J.10.4.2 Network Setup and Configuration Required for OOEMC Sync-Up Process, page J-41 for more information.

Step 5 If the trap IP address is not the issue, check whether there is an SNMP request failure. Normally, after the node resync process is triggered, ooemc will send SNMP requests to the switch to start the configuration upload file creation process. If the request fails, then ooemc will continue resending the SNMP requests until it exceeds the maximum number of retries and declares node resync failure with node mode equal to 5.

Note It should not take long to declare node resync failure because of the SNMP request failure. To verify that there is an SNMP failure, check the ooemc and snmpcomm log files.

Note Using ooemc10.6568.log as an example of an ooemc log filename, 10 is the child ID, the 6568 is the ooemc process ID. The child ID is calculated from the following formula: Remainder (NEDBACCSSID / number of ooemc child) + 1. To retrieve the process ID, use the CLI command **psg em**.

Step 6 Grep RESYNC from the log file. The grep result should include the node ID and node mode. Review the log messages in the log file to determine if an SNMP failure has occurred.

Step 7 Do the following:

a. Check the log file for trap 60903. If you find it, contact the platform team to investigate the bulk file creation failure on the switch.

   Very often, the node mode 2 problem is caused by a bulk file creation abort process on the switch. If there are no SNMP request failures, the switch should send traps 60901 and 60902 to ooemc. Trap 60901 indicates that the switch will start bulk file creation, while trap 60902 indicates bulk file creation done. When the ooemc receives a trap 60902, it will start to FTP the bulk file, which is a shelf generic configuration file. This is also the first file to be uploaded in every resync mode (coldstart, warmstart, or periodic resync.) The commonly seen mode 2 problem is that the switch will abort the bulk file creation and send trap 60903 to CTM. CTM will reschedule the next SNMP request unless it exceeds maximum retries.

b. Check the log file for trap 60902.

   CARD_01_CC.CF.10. This file is a shelf generic file and is the first file to be uploaded after CTM receives trap 60902 from the switch. The 10 is the node ID. If you find trap 60902 in the log file but no config file has been uploaded after a reasonable amount of time, it is possible that the FTP failed.

   To find out if FTP failure has occurred, do the following:

a. Grep “to ftp file" and the config filename, or just "FTP" from the log files.

b. Trace the log messages in the log file.

   For a more detailed information on SNMP request failure and FTP failure, check the snmpcomm and cwmftpd log files and the cwmftp.request_log. Search for the filename at the time the error happened in both files. The cwmftp.request_log gives the summary or final result of the FTP operation, and any error is reported. The cwmftp.log shows the FTP operation details.

CTM will upload and parse a set of config files from the switch. The following files are uploaded from the MGX NE, which contains VISM, AXSM, VXSM, SRM, and RPM/RPM-PR cards:

1. CARD_01_CC.CF
2. SM_1_slot#.CF
3. SM_1_slot#.CS
4. SM_CARD_01_slot#.CF
5. SM_CONN_01_slot#.CF
6. SM_ALARM_01_slot#.CF
7. SM_CON_UPDATE_01_slot#.CF
8. SM_CARD_01_SRM.CF

9. SM_CARD_01_RPM.CF
10. PNNI_01_CC.CF

Files 1 and 2 are uploaded for each NBSM. Files 4 to 7 are uploaded for each AXSM. File 9 is uploaded for all RPM/RPM-PR cards on the switch.

The following files are uploaded from the MGX NE. It includes VISM, AXSM, VXSM, SRM, RPM/RPM-PR, and RPM-XF cards:

1. CARD_01_CC.CF
2. SM_1_slot#.CF
3. SM_1_slot#.CS
4. SM_CARD_01_slot#.CF
5. SM_CONN_01_slot#.CF
6. SM_ALARM_01_slot#.CF
7. SM_CON_UPDATE_01_slot#.CF
8. SM_SC_slot#_transactionID_date.CF
9. SM_IC_slot#_transactionID_date.CF
10. SM_CARD_01_SRM.CF
11. SM_CARD_01_RPM.CF
12. PNNI_01_CC.CF

The difference between the items in these lists is in the files uploaded for AXSM cards and RPM-XF cards. For the switch software release 4.0 or later, the static file (SM_SC_slot#_transactionID_date.CF) and incremental file (SM_IC_slot#_transactionID_date.CF) are uploaded. For the switch software release 3.0 and earlier, conn, alarm, and conn update files are uploaded for each AXSM. Files 4 to 7 in the second list are uploaded for each RPM-XF card, and file 11 is uploaded for all RPM/RPM-PR cards on the switch.

Step 8 In another scenario in which the node mode stays in 2 for a very long time, the parsing of one particular config upload file has taken a very long time and has not completed. To view the parsing process, enter the following command:

```
tail -f <ooemc_log_file>
```

Step 9 Collect the ooemc, nts, snmpcomm, and cwmftpd log files from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.4.5 Node Resync Mode Is 5

Node mode 5 indicates that node resync has failed. This could be caused by the config upload or parsing failure of the shelf generic file (CARD_01_CC.CF.13, for example) or pnni file (PNNI_01_CC.CF.13, for example). In general, mode 5 signifies that a problem has happened in one or more stages of the entire resync process. The resync process is composed of the following stages and each stage alone can lead to mode 5 problems:

1. The ooemc triggers node resync.
2. The ooemc sends an SNMP request to the switch for bulk file creation.

3. The ooemc receives bulk file creation-related traps: 60901, 60902, and 60903.
4. The ooemc FTPs the config upload files from the switch after it has received 60901 and 60902 from the switch.
5. The ooemc parses the config upload files.
6. The ooemc declares sync-up done.

Step 1 Determine if the problem is caused by the SNMP request:

a. Grep RESYNC from the ooemc log files. The ooemc will change node mode to 2 when it starts the node resync process. You should see something like the following from the log:

```
NOTICE: N17 <EMC_Node_c::InSync> SENDING RESYNC STATUS 2 FOR NODE 17 TO GUI - Node is
synchronizing.
```

This message tells you that ooemc will start the node resync process for nodes with ID equal to 17 (N17). If you look further in the log, you should see log messages related to SNMP requests and SNMP responses. If the SNMP request is successful, the switch will respond to the request. The ooemc will then process the SNMP response by invoking response function, which may do nothing:

```
<EMC_SnmpFunc_c::ProcFunc_GenNodeBulkFile_1> entering
```

b. If the log messages indicate SNMP error, refer to the snmpcomm log files for more failure information.

Step 2 Determine if the problem is caused by bulk creation traps. Grep 60901, 60902, and 60903 from the log files. (See J.10.4.3 Node Mode Remains in 1, page J-41 for more information.) You should see something like the following:

```
INFO: <EMC_TrapClientImpl::onIncomingTrap> NTS NodeId 17 genericTrap 6 specificTrap 60901
INFO: <EMC_TrapClientImpl::onIncomingTrap> NTS NodeId 17 genericTrap 6 specificTrap 60902
```

Step 3 Determine if the problem is caused by the config file FTP. Check the FTP or the FTP plus config upload filename. You should see something like the following:

```
NOTICE: N17 <EMC_NodeFsmHandler_c::LoadShelf> to ftp /opt/svplus/tmp/CARD_01_CC.CF.17
INFO: <ParseFile_c::CheckFile> OOEMC9 CHECKSUM OK FOR FTP FILE
/opt/svplus/tmp/CARD_01_CC.CF.17
```

These messages indicate that FTP is successful and there is no checksum error in the file. From the log file, you should able to find out if there is an FTP problem. Refer to the cwmftpd log files for more failure information.

Step 4 Determine if the problem is caused by shelf generic file or pnni file parsing. After you have located where to do a checksum check on the shelf generic file (CARD_01_CC.CF.17, for example) or pnni file (PNNI_01_CC.CF.17, for example), continue to trace the log messages to see whether or not parsing error has occurred. If there are no errors, you should see the following:

```
INFO: N17 <EMC_NodeFsmHandler_c::FinishShelf> Parse /opt/svplus/tmp/CARD_01_CC.CF.17
successfully.
```

Defect information:

- Collect the ooemc, nts, snmpcomm, and cwmftpd log files from the /opt/svplus/log directory.
- Collect the config upload files from the /opt/svplus/tmp directory.

Possible alternative workaround—None.

J.10.4.6 CTM Database Is Inconsistent with Switch Data After Successful Coldstart (CTM Server Stop/Start) or Periodic Resync

After a successful node resynchronization triggered by the periodic resync, the CTM database is found to be inconsistent with the switch data.

Step 1 Collect the ooemc log files and all config upload files for the node. The ooemc implements a node-based cache. You can dump and save the cache.

Step 2 Get the process ID of the ooemc process that manages the node.

Step 3 Save the config upload files and ooemc log files.

Defect information—Collect the ooemc and config upload files from the /opt/svplus/log directory.

Possible alternative workaround: Manually resync the node. If the problem persists, perform a coldstart. If the problem is still not resolved, collect the log files and report the problem.

J.10.4.7 CTM CM GUI Shows Incomplete Connections After Successful Node Resync and Dbroker Sync-Up

CTM shows that some of connections are incomplete after the node resync process and dbroker synchronization process.

Step 1 Determine which ooemc process manages the node. The ooemc will manage the connection segment in the CTM database, which terminates on the MGX. Find the child ID of the ooemc process that manages your node. The purpose of finding the child ID of the ooemc process is to find the correct ooemc log files for inspection. The debugging process for this issue mainly focuses on log file inspection.

Step 2 After you have identified the ooemc log files, grep NotifyDataBroker from the files to see some log message examples before you modify your grep format. This will help you more efficiently grep the pair of log messages that correspond to the local and remote ends of one endpoint (primary endpoint or secondary endpoint) of a connection segment. In other words, each end (either primary end or secondary end) of a connection segment managed by ooemc should be logged with one pair of messages, one for local end and one for remote end. This pair of messages corresponds to one atm_connection segment entry in the database. Verify the information that ooemc sends to dbroker. Dbroker will refer to these messages from ooemc and construct a user_connection database entry. CTM Connection Management (CM) GUI displays connection information based on the user_connection database entry. Whether or not the connection is displayed as complete or incomplete depends on the information in the user_connection database entry. It is important to verify that ooemc sent the correct information to dbroker. Also verify that the segment database entries are populated correctly.

Step 3 If the correct number of messages have been forwarded to dbroker and the data in the messages is correct, but the user_connection database entry still contains invalid data, see J.10.13.2 Data Inconsistency, page J-129 for more debugging information, or contact the dbroker development engineer (DE) for further investigation. If the problem is due to wrong data populated in segment database entries, then the EM DE should look at the problem.

Defect information:

- Collect ooemc and dbroker log files from the /opt/svplus/log directory.

- Collect config upload files from the /opt/svplus/tmp directory.

Possible alternative workaround is to manually resync the node. If the problem persists, perform a coldstart. If the problem is still not resolved, collect the log files and report the problem.

J.10.4.8 CTM GUI Shows Mismatched Information Between GUI Views and Database Data

After an initial ooemc node resync, such as a coldstart process, GUI views such as Network Monitor tree view, Inspector View, and Chassis View display information that does not match newly provisioned or updated database data. The problem persists even after each subsequent manual or periodic resync.

Step 1 Determine which ooemc process manages the node and find the child ID of the ooemc process that manages your node. The purpose of finding the child ID of the ooemc process is to find the correct ooemc log files for inspection. The debugging process for this issue mainly focuses on log file inspection.

Step 2 Initiate an initial node resync, such as coldstart. Ooemc starts sending newly provisioned or updated database data to the network management (NM) server. The current supported database tables for NM server message forwarding include the following:

- node
- card
- line
- ausm_port
- cesm_port
- frp
- rpm_port
- svc_port
- virtual_port
- aps
- ima_group
- ima_link
- linedistribution
- au4tug3
- controller
- license_in_use
- mfr_bundle
- mfr_link
- peripheral
- redundantcard
- sensor

Step 3 To determine whether or not ooemc sent newly provisioned or updated database data to the NM server, grep ComposeNMSMsg from the ooemc log files. The key words in log messages that correspond to the supported database tables in step 2 are the following:

- EMC_DBProperty_Node_c::ComposeNMSMsg

- EMC_DBProperty_Card_c::ComposeNMSMsg
- EMC_DBProperty_Line_c::ComposeNMSMsg
- EMC_DBProperty_AusmPort_c::ComposeNMSMsg
- EMC_DBProperty_CesmPort_c::ComposeNMSMsg
- EMC_DBProperty_FrPort_c::ComposeNMSMsg
- EMC_DBProperty_RpmPort_c::ComposeNMSMsg
- EMC_DBProperty_SvcPort_c::ComposeNMSMsg
- EMC_DBProperty_VtPort_c::ComposeNMSMsg
- EMC_DBProperty_Aps_c::ComposeNMSMsg
- EMC_DBProperty_ImaGroup_c::ComposeNMSMsg
- EMC_DBProperty_ImaLink_c::ComposeNMSMsg
- EMC_DBProperty_LineDist_c::ComposeNMSMsg
- EMC_DBProperty_AU4TUG3_c::ComposeNMSMsg
- EMC_DBProperty_Ctrlr_c::ComposeNMSMsg
- EMC_DBProperty_LicenseInUse_c::ComposeNMSMsg
- EMC_DBProperty_MfrBundle_c::ComposeNMSMsg
- EMC_DBProperty_MfrLink_c::ComposeNMSMsg
- EMC_DBProperty_Peripheral_c::ComposeNMSMsg
- EMC_DBProperty_RedCard_c::ComposeNMSMsg
- EMC_DBProperty_Sensor_c::ComposeNMSMsg

Note Database data will not be sent to NMServer during the initial node resync. It is after the initial resync that ooemc starts sending updated or newly provisioned database data to NMServer. Each ooemc log message from grep contains detailed information on the identity of the NE object and the required fields from the corresponding database table. The following is an example of NMServer message for line tables:

```
ooemc10.24370.log.old.5:( 24370: 4) 23:15:17 INFO: N0:C7:B2:L2
<EMC_DBProperty_Line_c::ComposeNMSMsg> (MODIFY::LINE) aNMSEvent.node:0 type:4 subType:1
lpbkType:1 alarmState:1 adminState:1 sectStatus:6 pathState:2
```

In this example, the identity of the NE object is N0:C7:B2:L2, which is the line with node ID=0, slot=7, bay=2, and line#=2. The database operation is update. The rest of the message shows the values of the required fields from the line table.

Step 4 If grep returns log messages that indicate matched data, then you need to continue investigation on the NM server. See J.10.5.1 CTM Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Basics, page J-53 for information on nmController.

Defect information—Collect ooemc and NMServer log files from the /opt/svplus/log directory.

Possible alternative workaround—Manually resync the node. If the problem persists, perform a coldstart. If the problem is still not resolved, collect the log files and report the problem.

J.10.4.9 CTM Database and Switch Data Inconsistency Issues After Node Provisioning for MGX

This section includes the following information:

- J.10.4.9.1 Database Table Population Through Traps and SNMP Upload, page J-49
- J.10.4.9.2 Switch Data Does Not Match CTM Database Table After Node Provisioning, page J-49

J.10.4.9.1 Database Table Population Through Traps and SNMP Upload

Except for node and/or card resync, another mechanism that CTM ooemc uses to populate the database table entries is through trap processing followed by SNMP upload, if necessary. You can provision the switch through switch CLI, CTM GUI, or CTM service agents. All three cases will involve trap processing and SNMP upload on ooemc. Only connections can be provisioned by the CTM CM GUI. Other provisioning, such as line and port, have to go to CTM service agents. The MGX switch CLI can do all.

J.10.4.9.2 Switch Data Does Not Match CTM Database Table After Node Provisioning

After switch provisioning through the switch CLI, CTM GUI, or CTM service agents, the switch data does not match the CTM database.

Step 1 If the issue is caused by a trap (for example, if you provision a connection on a switch or through CTM GUI or service agent, and CTM does not populate the database entry or the information in the database entry does not match the switch data), it is possible that CTM did not receive the trap, or that it received the trap but the trap is buffered in the ooemc trap queue, and trap processing has been delayed. On the other hand, if the data in the CTM database is not correct, it is also possible that the SNMP upload failed to upload correct data. Study the log files to understand the root cause of the inconsistency problem.

Step 2 To determine whether or not a trap has been received and processed, there are key words in the ooemc log files that you can grep. For example, to find out the channel traps from node_id=4, slot=6, vpi=1, and vci=326, you can grep "TRAPLIST" as shown in the following:

```
cwmult60% grep "TRAPLIST: N4:" ooemc* | grep "Channel Trap" | grep "C6" | grep "vpi 1 vci
326"
ooemc10.5760.log.old.55:( 5760: 10) 23:21:12 INFO: TRAPLIST: N4: Channel Trap 60310 from
C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2 operS 1 alarm 67
ooemc10.5760.log.old.55:( 5760: 10) 23:21:12 INFO: TRAPLIST: N4: Channel Trap 60310 <
PROCESSED > from C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2
operS 1 alarm 67
ooemc10.5760.log.old.73:( 5760: 10) 23:23:48 INFO: TRAPLIST: N4: Channel Trap 60310 from
C6 B2 L1 P20 Ch299 ifIndex 17176597 vpi 1 vci 326 upCntr 0 vpcFlag 2 operS 1 alarm 66
```

For other kinds of traps, you can use the following key words to supplement "TRAPLIST" in your grep statement:

- Port Trap
- RscPart Trap
- Svc Trap
- SonetLn Trap
- SctCard Trap
- SonetPath Trap
- FunMod Trap
- LineMod Trap

- RedCard Trap
- TrapMiss Trap
- VsiCtrlr Trap
- DS3Line Trap
- AtmPhy Trap
- Peripheral Trap
- CoreSwth Trap
- TrapLost Trap
- AtmAddr Trap
- Restart Trap
- Node Trap
- SonetAps Trap
- LMIPort Trap
- Pnni IF Trap
- Bulkfile Trap
- Vism Trap
- Vism Ann Trap
- SubIf Trap
- NBSMCnfg Trap
- NBSMChan Trap
- NBSMLine Trap
- AusmLine Trap
- AusmPort Trap
- AusmChan Trap
- AusmIma Trap
- FrChan Trap
- FrPort Trap
- CesmPort Trap
- CesmChan Trap
- HsFrPort Trap
- HsFrChan Trap
- LineDist Trap
- DS3Path Trap
- Chan Upload
- Party Trap
- PrefRoute Trap
- CardIma Trap
- DS1 Line Trap

- SctPort Trap
- SvcDerouteGroomTrap
- Channel Trap
- TUG3Path Trap
- Cug Trap
- AddrCug Trap
- RSC Upload
- APS Upload
- FrPort State Upload
- MPSM Upload
- Vism ToneDetect Trap
- License Trap
- PortAtmIf Trap
- VxsmPvcRed Trap
- ChanProt Trap
- VxsmGwDsp Trap
- VxsmGwIp Trap
- VxsmGw Trap
- VxsmSysRes Trap
- VxsmGw1 Trap
- VxsmMgc Trap
- VxsmMgcIp trap
- VxsmMgcGrpParam Trap
- VxsmMgcGrpMgc Trap
- VxsmMgcGrpProt Trap
- VxsmAal2Prof Trap
- VxsmCodec Trap
- VxsmSvc Trap
- VxsmAal2CrossConn Trap
- VxsmAal25DataProfileTrap
- VxsmSensor Trap
- VxsmSensorThrhd Trap
- VxsmModule Trap
- DS0Grp Trap
- VxsmAnnounce Trap
- VxsmAudioFile Trap
- VxsmDs0XConn Trap
- VxsmMegaco Trap

- VxsmCrr Trap
- VxsmTone Trap
- VxsmAs Trap
- VxsmAsp Trap
- VxsmAs Trap
- VxsmLapd Trap
- VismABCDBitTemplate Trap

Review the log messages using the **traplist** command and decide how you can grep the messages according to your needs. In the above example, there is another key word ("PROCESSED") that indicates that the trap has been processed. This gives you the starting point in the log file so that you can study the log messages. If the database is not populated correctly, then the subsequent log messages should provide you information on the database inconsistency problems. Some trap processing may invoke SNMP data upload. From the log messages, you can verify whether the uploaded data is correct or not. Other possible reasons for database inconsistency are:

- SNMP upload failure and maximum retries is exceeded; SNMP timeout; or throttle error. You can verify the problem in the snmpcomm log files.
- Database operation error. You can verify the problem in the ooemc log files.

If you do not know exactly what trap sequence is sent by the switch to CTM, you should try a working scenario and study the log for the trap sequence, or you can use HPOV to determine the trap sequence.

Step 3 To verify whether or not a trap has been received from the switch and forwarded to ooemc, refer to the nts log. If the trap has been buffered in the trap queue, the possible reasons are:

- Node is syncing due to regular node resync or due to -2 trap.
- Card is syncing and the trap is related to the card. The traps will be buffered in the queue until card resync completes.
- Summary alarm trap is processed. Summary alarm is being uploaded or parsed. You can grep the log files for information related to summary alarm traps.

To verify that the trap has been put into the queue, you can do the following:

```
grep EMC_TrapQueue_c::append ooemc_log | grep trap_num
```

You should see something like the following:

```
INFO: <EMC_TrapQueue_c::append> entering. ======> append trap# 60303 to trap queue;
getHdlrLevel=5, getTrapLevel=5, #=174
```

Defect information—Collect ooemc, nts, and snmpcomm log files from the /opt/svplus/log directory.

Possible alternative workaround—Manually resync the node. If the problem persists, perform a coldstart. If the problem is still not resolved, collect the log files and report the problem.

J.10.5 Configuration Center, Chassis View, Diagnostics Center, and Statistics Report Problems

This section includes the following information:

- J.10.5.1 CTM Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Basics, page J-53
- J.10.5.2 Basic Issues, page J-55
- J.10.5.3 Topology Discovery Issues, page J-56
- J.10.5.4 Network Element Discovery Issues, page J-59
- J.10.5.5 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Alarm Issues, page J-62

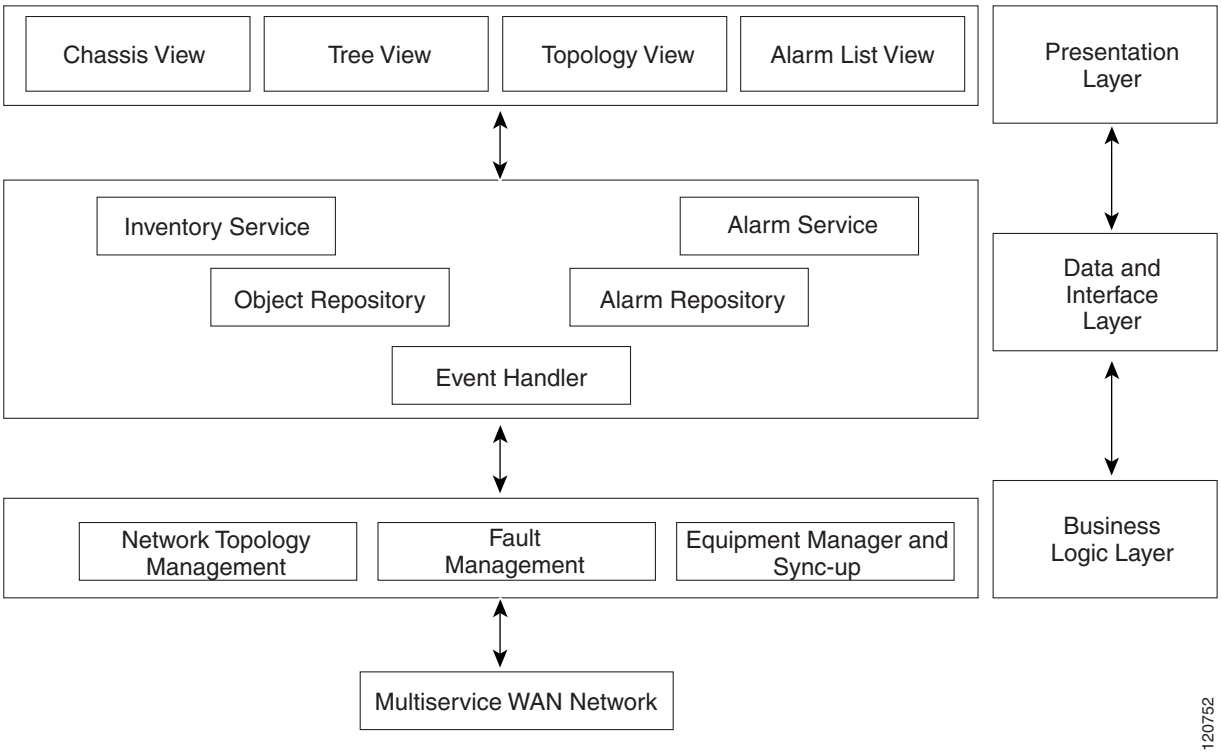
J.10.5.1 CTM Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Basics

CTM manages MGX NEs. The topology module discovers the nodes and trunks. Once the nodes are discovered, the EM module syncs up with the nodes to discover the card, line, port, and so on. All the discovered nodes, trunks, and node elements are published by NMServer and are displayed in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report. The Configuration Center, Chassis View, Diagnostics Center, or Statistics Report have the tree view and Inspector View. The tree view and Inspector View feed off the data published by NMserver.

CTM is notified of all subsequent changes in the network through traps.

Figure J-1 shows the end-to-end architecture.

Figure J-1 CTM End-to-End Architecture



NMServer provides inventory and alarm information for the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report. The node information is pushed by topod to NMServer. The initial inventory of card, lines, ports, and so on, is read from the database. The dynamic updates are pushed to NMServer from topod, ooemc, and sdbroker.

There are two utilities under the /opt/svplus/util/ directory that are shipped with CTM to debug issues in NMServer:

- nmControl—This utility provides the means to check the NMServer cache and its state. Output is redirected to /opt/svplus/log/nmControl.log. Cache dumps are redirected to /opt/svplus/log/nmControl.dump. The utility allows the following operations, all of which are nondestructive and perform the tasks in a passive mode.

Note Do not use the All Cache operation to dump the cache for a large network that has more than 1000 nodes.

  - Resync Node—Resyncs the node (specified by the node_id).
  - All Cache—Dumps all the data in its cache to the dump file.
  - Topology Cache—Dumps topology (node) data to the dump file.
  - Node Cache—Dumps a node's data (specified by node_id) to the dump file.
  - CTM Alarm Cache—Dumps the CTM-specific alarms to the dump file.
  - Client Manager Cache—Dumps the information about all the clients to the dump file.
  - Error Statistics—Dumps the error information associated with the sync-up to the dump file.
  - Sync-Up Status—Dumps the sync-up state to the dump file.

  - Configuration—Dumps the configuration data to the dump file.

- nmClient—This utility is used to isolate an issue between client and server. It is used to query the NMServer the same way as the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report GUI queries the server. Output is redirected to /opt/svplus/log/nmClient.log. Cache dumps are redirected to /opt/svplus/log/nmClient.dump.

  You must perform the Register Client operation before performing any other operations. When you are finished using the client, perform the Unregister Client operation.

  - Register Client—Registers with the server.
  - Update Filter—Updates the subscription/filter with the server passing the FDN.
  - Unregister Client—Unregisters with the server.
  - Get Topology—Gets the topology information of networks and nodes.
  - Get Children—Gets the list of children for a particular object in the tree.
  - Get CwmInfo—Gets the CTM sync-up state information.
  - Get ManagedObject—Gets the detailed information about an object in the tree.
  - Subscribe for all events—Subscribes to all updates on the server.
  - Unsubscribe for all event—Unsubscribes from all updates on the server.

The GUI client's log files (CMSCclient.log) are saved under log directories; for example, in Windows, D:Documents and Settings\<username>\log\, or in Unix: /opt/svplus/log.

J.10.5.2 Basic Issues

This section includes the following information:

- J.10.5.2.1 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show Any Nodes, page J-55
- J.10.5.2.2 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Is Unable to Connect to Server, page J-56
- J.10.5.2.3 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Newly Added Node, page J-56

J.10.5.2.1 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show Any Nodes

Step 1 Check whether the nodes are discovered. See J.10.2.1 No Nodes Are Discovered, page J-34.

Step 2 Check whether NMServer has the nodes and trunks in its cache. This can be done by using the command **nmControl** in the CTM CLI.

Step 3 If the nodes are in the NMServer cache, open a new GUI and verify whether the nodes are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report GUI.

J.10.5.2.2 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Is Unable to Connect to Server

Step 1 Check whether the client registers in NMServer.log.

Step 2 Enable orbix logs by creating the orbix directory in /opt/svplus/log/ directory.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log, NMServer.log
- Orbix logs

Possible alternative workaround—None.

J.10.5.2.3 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Newly Added Node

Step 1 Check whether the nodes have been discovered. See J.10.2.1 No Nodes Are Discovered, page J-34 for more information.

Step 2 Check whether NMServer has the nodes in its cache. This can be done by using the command **nmControl** in the CTM CLI.

Step 3 If the nodes are in the NMServer cache, open a new GUI and verify whether the nodes are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workaround—Open a new GUI.

J.10.5.3 Topology Discovery Issues

This section includes the following information:

- J.10.5.3.1 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Node, page J-57
- J.10.5.3.2 Node Information Incorrect on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-57
- J.10.5.3.3 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows a Node that Is Not in the Network, page J-57
- J.10.5.3.4 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows Incorrect SyncState for a Node, page J-58
- J.10.5.3.5 Duplicate Nodes Are Displayed on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-58

J.10.5.3.1 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Node

Step 1 Check whether the nodes are discovered. See J.10.2.1 No Nodes Are Discovered, page J-34 for more information.

Step 2 Check whether NMServer has the nodes in its cache. This can be done by using the command **nmControl** on the CTM CLI.

Step 3 If the nodes or trunks are in the NMServer cache, open a new GUI and verify whether the nodes are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

J.10.5.3.2 Node Information Incorrect on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

Step 1 Check the node information in the database using **selnd** command.

Step 2 Check the node information in the NMServer's cache. This can be done by using the **command nmControl** on the CTM CLI.

Step 3 Check the CMSCclient.log for the node information.

Step 4 From nmClient, use the getTopology option to retrieve the node information and verify whether it matches the database and the GUI.

Step 5 If the node information is correct in the NMServer cache, open a new GUI and verify whether the node is shown correctly in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- selnd o/p
- nmControl.dump
- CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

J.10.5.3.3 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows a Node that Is Not in the Network

Step 1 Check the node information in the database by querying the node, packet_line table. Verify whether the node is active.

Step 2 If the node is active, see J.10.2.1 No Nodes Are Discovered, page J-34.

Step 3 Check the node in the NMServer's cache. This can be done by using the command **nmControl** in the CTM CLI.

Step 4 Check the CMSCclient.log for the node/trunk. Verify whether a delete message was received for the node.

Step 5 From nmClient, use the getTopology option to retrieve the node information and verify whether it matches the database and GUI.

Step 6 If the node is not present in the NMServer cache, open a new GUI and verify whether the node is shown in it.

Defect Information—Collect the following information for further analysis:

- ILMITopoc.log, topod.log, and NMServer.log.
- Dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Output of the switch CLI, selnd, and dbnds.

J.10.5.3.4 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows Incorrect SyncState for a Node

---

Step 1 Check the node information in the database by querying the node table. This can be done by using the command **selnd** on the CTM CLI. Check the status.

Step 2 Check the node in the NMServer's cache. This can be done by using the command **nmControl** on the CTM CLI.

Step 3 Check the CMSCclient.log for the node. Verify whether the correct message was received for the node.

Step 4 From nmClient, use the getTopology option to retrieve the node information and verify whether it matches the database and the GUI.

Defect Information—Collect the following information for further analysis:

- ILMITopoc.log, topod.log, and NMServer.log.
- Dump outputs of ILMITopoc, topod and NMServer. The dump can be captured by issuing a kill -USR1 signal to the process.
- Output of the switch CLI, selnd, and dbnds.

J.10.5.3.5 Duplicate Nodes Are Displayed on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

---

Step 1 Check whether the node table has duplicate node IDs.

The node table can be queried using the following command:

tballraker18% echo "select (*) from node where node_id=2 and slot=1" | dbaccess stratacom

Step 2 Check whether both nodes in the database have active=1. If both nodes are active then collect the logs.

Step 3 If duplicate nodes do not exist in the database, check the cache of NMServer using **nmControl**.

Step 4 Check the CMSCclient.log for the node.

Step 5 From nmClient, use the getTopology option to retrieve the node information and verify whether it matches the database and the GUI.

Step 6 If duplicate nodes are not present in the NMServer cache, open a new GUI and verify whether the node is shown in it.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under /opt/svplus/log. For PC Client, collect CMSCclient.log file under D:\Documents and Settings\<username>\log.
- Node data from node table for that specific node.
- ILMITopoc.log and topod.log, if there are duplicate nodes in the database.

Possible alternative workaround—None.

J.10.5.4 Network Element Discovery Issues

This section includes the following information:

- J.10.5.4.1 All the Cards Under a Node Are Missing, page J-59
- J.10.5.4.2 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Card, Line, or Port for a Node, page J-60
- J.10.5.4.3 Card, Line, or Port Information Is Incorrect on Configuration Center, Chassis View, Diagnostics Center, or Statistics Report, page J-60
- J.10.5.4.4 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows a Card, Line, or Port that Is Not Present in a Node, page J-61

J.10.5.4.1 All the Cards Under a Node Are Missing

No cards are shown under a node in the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

Step 1 Check whether the node is synced up. This can be done by using the command **selnd** on the CTM CLI.

Step 2 If the node has not synched up, wait for it to do so.

Step 3 If the node has synced up, check whether cards are populated in the card table. If the card table is empty, collect the EM logs. See J.10.4 Equipment Management Problems, page J-40 for more information.

Step 4 Check whether NMServer has cards in its cache. This can be done by using the command **nmControl** on the CTM CLI.

Step 5 If cards are not present in the NMServer cache, collect the logs.

Step 6 If cards are present in the NMServer cache, use nmClient and verify whether getChildren for node's FDN returns the cards in the nmClient.<pid>.dump file.

Step 7 If cards are present in the NMServer cache, open a new GUI and verify whether the cards are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.
2. Use nmControl and perform "Resync Node," specifying the node ID.

J.10.5.4.2 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Does Not Show a Card, Line, or Port for a Node

Step 1 Check whether the node is synced up. This can be done by using the command **selnd** on the CTM CLI.

Step 2 If the node has not synced up, wait for it to do so.

Step 3 If the node has synced up partially, check whether the card, line, or port is populated in the database. Refer to the *Cisco Transport Manager Release 6.0 Database Schema*.

Step 4 If the entry is not populated in the database, see J.10.4 Equipment Management Problems, page J-40.

Step 5 If the entry is present in the database, check the NMServer cache. This can be done by using the command **nmControl** on the CTM CLI. Check the nmControl.<pid>.dump

Step 6 If the element is not present in the NMServer cache, use nmClient and verify whether getChildren for FDN returns the entities in the nmClient.<pid>.dump file.

Step 7 If the element is present in the NMServer cache, open a new GUI and verify whether the missing elements are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.
2. Use nmControl and perform "Resync Node," specifying the node ID.

J.10.5.4.3 Card, Line, or Port Information Is Incorrect on Configuration Center, Chassis View, Diagnostics Center, or Statistics Report

The entity information of an element shows incorrectly on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

Step 1 Check whether the node is synced up. This can be done by using the command **selnd** on the CTM CLI.

Step 2 If the node has not synced up, then wait for it to do so.

Step 3 Check whether the card, line, or port is populated in the database. Refer to the *Cisco Transport Manager Release 6.0 Database Schema*.

Step 4 If the entry in the database matches the GUI, see J.10.4 Equipment Management Problems, page J-40.

Step 5 If the entry doesn't match the database, check the NMServer cache. This can be done by using the command **nmControl** on the CTM CLI. Check the nmControl.<pid>.dump.

Step 6 Use nmClient and verify whether getChildren for FDN returns the correct information for the element in the nmClient.<pid>.dump file.

Step 7 If the element is present in the NMServer cache, open a new GUI and verify whether the missing elements are shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.
2. Use nmControl and perform "Resync Node," specifying the node ID.

J.10.5.4.4 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Shows a Card, Line, or Port that Is Not Present in a Node

An extra card, line, or port element is shown incorrectly on the Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

Step 1 Check whether the node is synced up. This can be done by using the command **selnd** on the CTM CLI.

Step 2 If the node has not synced up, then wait for it to do so.

Step 3 Check whether the card, line, or port is populated in the database. Refer to the *Cisco Transport Manager Release 6.0 Database Schema*.

Step 4 If the element is present in the database but does not match what is shown in the GUI, see J.10.4 Equipment Management Problems, page J-40.

Step 5 If element is not in the database, check the NMServer cache. This can be done by using the command **nmControl** on the CTM CLI. Check the nmControl.<pid>.dump.

Step 6 Use nmClient and verify whether getChildren for FDN returns the element in the nmClient.<pid>.dump file.

Step 7 If element is not present in the NMServer cache, open a new GUI and verify whether the extra element is shown in it.

Defect Information—Collect the following information for further analysis:

- topod.log, ILMITopoc.log, and NMServer.log
- nmControl.dump
- CMSCclient.log

Possible alternative workarounds:

1. Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report GUI.
2. Use nmControl and perform Resynch node, specifying the node ID.

J.10.5.5 Configuration Center, Chassis View, Diagnostics Center, or Statistics Report Alarm Issues

This section includes the following information:

- J.10.5.5.1 Alarm Processing Basics, page J-62
- J.10.5.5.2 XML Schema for Alarm Rules, page J-63
- J.10.5.5.3 Alarm Severity and Object Severity, page J-65
- J.10.5.5.4 Severity Shown on Tree View Does Not Match Severity Shown on Platform, page J-66
- J.10.5.5.5 Alarm List Shows Alarm that Does Not Exist on Platform, page J-67
- J.10.5.5.6 Transient Event Has Disappeared Unexpectedly, page J-68
- J.10.5.5.7 Port in Tree View Displays Aggregate Alarm; However, No Children Exist Under Port, page J-68

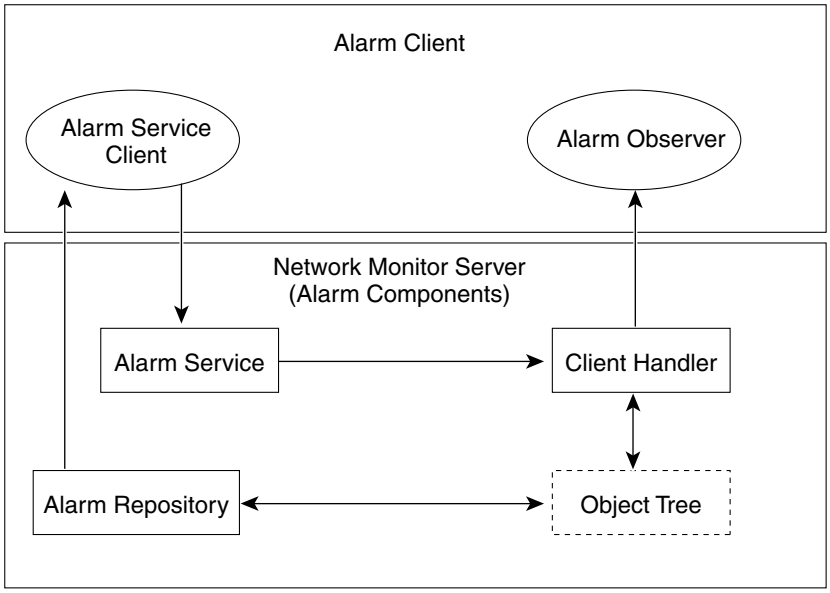
J.10.5.5.1 Alarm Processing Basics

Alarm processing is done within the NMServer processes. The following are some vital points with regard to alarm processing:

- Alarm rules are defined in an XML file (/opt/svplus/xml/ruledata.xml). For details on XML schema alarm rules, see Figure J-2.
- GUI clients register for alarms by providing the parent FDN.
- GUI clients pull initial alarms from NMServer. After initial pull of alarms, all alarms are pushed to registered clients by NMServer when alarms occur.
- Object severity for any and all network elements is determined by the XML alarm rule.
- Administrative states of network element states are not displayed in the alarm list, only alarm states.
- Alarm List displays mostly active alarms, however some events are also displayed. For details on events versus alarms, see J.10.5.5.2 XML Schema for Alarm Rules, page J-63.
- Some alarms result in the network element having a different alarm severity then the actual alarm. For details on object severity versus alarm severity, see J.10.5.5.3 Alarm Severity and Object Severity, page J-65.

Alarms for various network elements are stored in memory cache in the NMServer Object Tree. GUI clients register for alarms from NMServer by providing the FDN of the network element for which they would like alarms. All alarms for network elements under the FDN registered will be sent if the parent FDN is registered. GUI clients may also update alarms, for example by flagging an alarm as acknowledged or manually clearing an alarm. These updates are done through the Alarm Repository component of NMServer. Figure J-2 illustrates the client/server architecture for alarm components in NMServer.

Figure J-2 Client/Server Architecture for Alarm Components



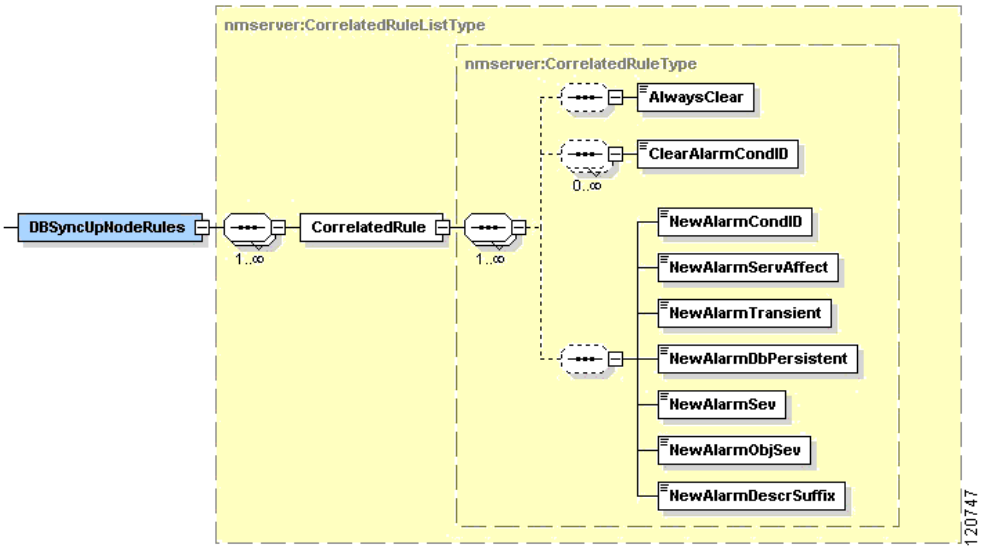
J.10.5.5.2 XML Schema for Alarm Rules

Alarm rules are defined in XML, specifically, in a file named $HOME/xml/ruledata.xml. These alarm rules are read once when NMServer starts. When events are processed, the rules are queried from memory to determine what action, with regard to alarms, should be taken on the event. There are three types of alarm rules defined in the XML schema: Correlated, Correlated Bitmap, and Transient. Specifics on each of these three types are as follows.

1. Correlated Alarm Rule Type

The correlated alarm rule type is the most common in ruledata.xml. This rule is used when a network element can be in only one of many states at any one time. If the entity were to change states, then the previous alarm state would be cleared. Most network elements managed by CTM fall into this category. A simple example is the database sync-up status of a node. The sync-up status can be one of Partial Sync-Up, Sync-Up Failed, or In Sync. Any one of these states correlates out any other. See Figure J-3.

Figure J-3 Correlated Alarm Rule Diagram



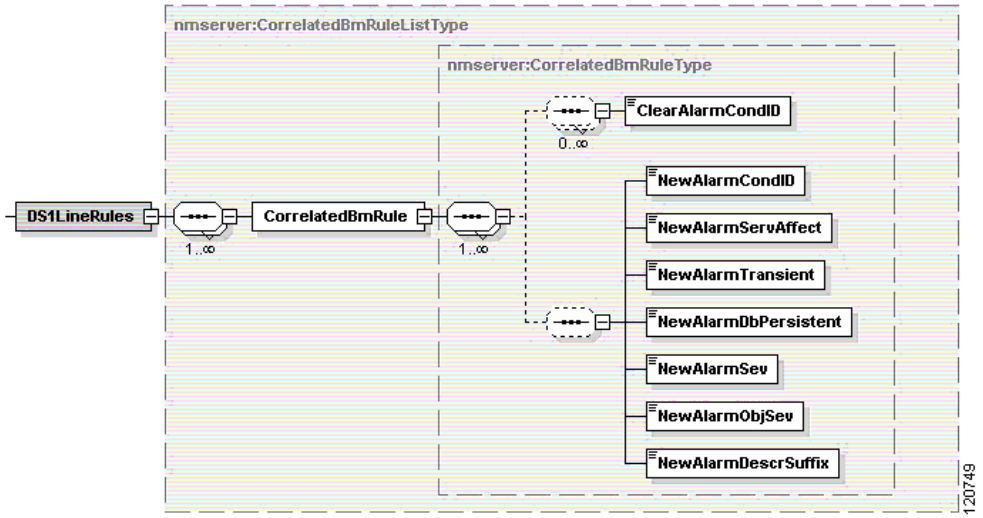
A CorrelatedRule can have any of the following:

- 1 AlwaysClear (Used when a given element never has an alarm, such as in a top-level network)
- 0 or more ClearAlarmCondIds
- 1 new alarm (which consists of NewAlarmConditionID, NewAlarmServAffect, and so on.)

2. Correlated Bitmap Alarm Rule Type

The correlated bitmap alarm rule type is different from the correlated alarm rule type because the bitmap rule type can represent the many states an entity can be in at any one particular time. The correlated bitmap rule type is used primarily to represent line alarms. Lines can have many different alarms associated with them at any given time, such as Loss of Signal and Loss of Frame. See Figure J-4.

Figure J-4 Correlated Bitmap Alarm Rule Diagram



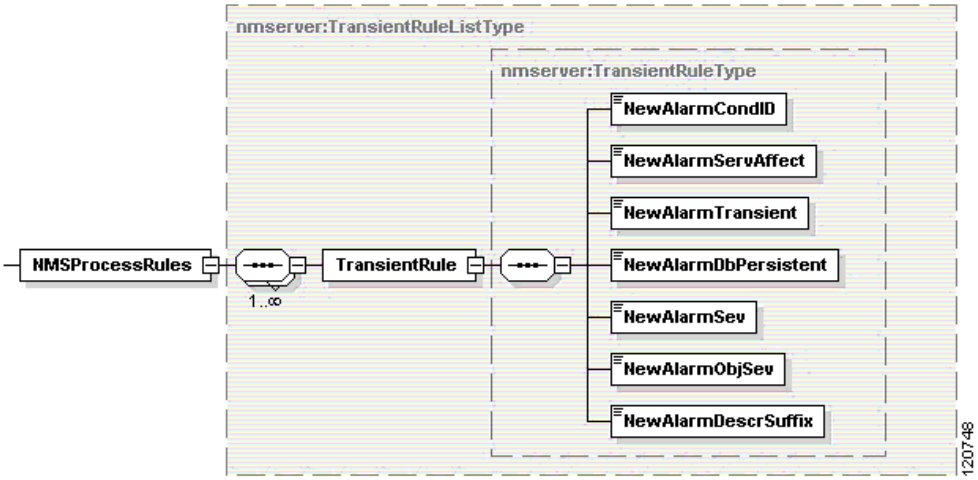
A CorrelatedBmRule can have any of the following:

- 0 or more ClearAlarmCondIds
- 1 new alarm (which consists of NewAlarmConditionID, NewAlarmServAffect, and so on)

3. Transient Alarm Rule Type

The transient alarm rule type is used to distinguish events from alarms. The alarm list shows some events. Events are normally associated with the NMS itself. Examples of events are Process Restarted or Primary Gateway Disconnected. These are NMS events that are not correlated, but are displayed in the alarm list. Another example of a transient event that is not related to the NMS is a card switchover. If automatic protection switching (APS) is enabled on a card and there is an APS switchover, an event will be displayed in the alarm list. The primary distinction between transient events and correlated alarms is that transient events are not cleared by the network, whereas correlated alarms are. See Figure J-5.

Figure J-5 Transient Alarm Rule Diagram



A transient alarm rule can have only one new alarm associated with it.

Note There is no ClearAlarmCondID associated with a transient rule. Transient alarms can be manually cleared by the user, cleared by the same transient alarm occurring twice, or purged by NMServer when a high threshold is hit.

J.10.5.5.3 Alarm Severity and Object Severity

Every alarm in an alarm rules XML file is assigned two severities: object and alarm. The two severities are called Object and Alarm severity. These severities do match for most alarms. There are some cases, however, where these severities are different. The following is an example of an XML alarm rule where object and alarm severity do not match:

```
<CorrelatedRule State="1 -1">
<ClearAlarmCondID>10302</ClearAlarmCondID>
<ClearAlarmCondID>10303</ClearAlarmCondID>
<ClearAlarmCondID>10304</ClearAlarmCondID>
<NewAlarmCondID>10301</NewAlarmCondID>
<NewAlarmServAffect>0</NewAlarmServAffect>
<NewAlarmTransient>0</NewAlarmTransient>
<NewAlarmDbPersistent>0</NewAlarmDbPersistent>
```

```
<NewAlarmSev>6</NewAlarmSev>
<NewAlarmObjSev>7</NewAlarmObjSev>
<NewAlarmDescrSuffix>Sync-Up has not started yet</NewAlarmDescrSuffix>
</CorrelatedRule>
```

This alarm will occur if the southbound processes (EMs) send a node message with EM sync-up status as 1 or -1. If that does occur, then the node should be unreachable severity (value 7) in the tree view. Note that there is no unreachable severity in the alarm list. This is why there are two severities for each alarm. Unreachable alarms have Critical (value 6) severity in the alarm list.

Another instance when alarm and object severity do not match is for aggregate port alarms. Aggregate port alarms are alarms that summarize the condition of the connections on the port. Since these alarms should not affect the severity of the port, the object severity of these is alarms is Clear (value 3). The following is the XML for an aggregate port alarm:

```
<CorrelatedBmRule StateBm="1">
<NewAlarmCondID>40801</NewAlarmCondID>
<NewAlarmServAffect>0</NewAlarmServAffect>
<NewAlarmTransient>0</NewAlarmTransient>
<NewAlarmDbPersistent>1</NewAlarmDbPersistent>
<NewAlarmSev>5</NewAlarmSev>
<NewAlarmObjSev>3</NewAlarmObjSev>
<NewAlarmDescrSuffix>Aggregate Port alarm, One or more connections on this port are in
primary failure</NewAlarmDescrSuffix>
</CorrelatedBmRule>
```

Note The alarm severity (NewAlarmSev tag) is Major (value 5).

J.10.5.5.4 Severity Shown on Tree View Does Not Match Severity Shown on Platform

Severity of a network element in tree view does not match the severity the switch is showing for the same network element.

Step 1 Verify whether the customer is comparing the correct severity icon.

- **a.** There are two severities associated with every object in the tree view, the aggregate severity and the self severity. The aggregate severity is on the left, the self severity is on the right. Since the switch does aggregation of many faults, the customer should compare the aggregate severity of the object in the tree view with the severity of the switch.
- **b.** If you are looking at the correct severity icon and there is still a discrepancy between the severities, continue to step 2.

Step 2 Verify whether CTM has synced up with the node.

- **a.** Log in to the CTM server and type **selnd**.
- **b.** Verify that the node mode in question is 3.

Step 3 If the mode is 3, verify whether the discrepancy is caused by aggregated connection alarms. NMServer does more aggregation of alarms than the platform. For instance, NMServer aggregates connection alarms up the port and the switch does not. Therefore, if the tree view displays a higher severity then the switch, it may be caused by one or more aggregated port alarms.

- **a.** Right-click the NE in the tree view and choose **show alarms**. All of the alarms for this NE and its children should appear in the alarm list.
- **b.** Filter on the alarms that have greater severity then what the platform is showing.

c. Verify whether or not the alarms are aggregate port alarms. If so, this is expected behavior and there is no defect. If there are alarms that have greater severity then what is shown on the platform, and they are not aggregate port alarms, continue to the next step to see whether the alarm is in the database.

Step 4 Verify whether the database has the correct alarm state. Refer to the *Cisco Transport Manager Release 6.0 Database Schema* for information on what table to look up for this particular entity type.

Defect Information—Collect the following information for further analysis:

- NMServer.log
- nmControl.dump
- CMSCclient.log on client machine

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

J.10.5.5.5 Alarm List Shows Alarm that Does Not Exist on Platform

There are several alarms that are correlated by NMServer and are not handled by the switch. This is the case because the NMS keeps track of alarm conditions that may not be relevant to the switch alone, but are relevant to the switch and the NMS. One example of such an alarm is the node sync-up state. The switch itself is not interested in the fact that the NMS may not be synced up with it, but the NMS is interested in this information. Therefore if the node is still syncing up with the NMS, an alarm will be displayed for this node in the alarm list, but there will not be such an alarm on the platform. The following is a summary of alarms that may be seen in the alarm list, but not on the platform.

Step 1 If there is an alarm in the alarm list, and not on the platform, see if the suspect alarm is included in the following list:

- Node sync-up status alarms
- Node database sync-up status alarms
- Node Management State status alarms
- Node Aggregate alarm status
- Link0/Link1 Node alarms
- Card sync-up status alarms
- Aggregate Port (Connection) alarms

Step 2 If the suspect alarm is not included in any of the alarm list mentioned in step 1, it may be a defect. Perform the following:

a. Verify whether the database has the correct alarm state. See the *Cisco Transport Manager Release 6.0 Database Schema* for information on what table to look up for this particular entity type.

b. Collect the following information:

- topod.log, linktopoc.log, ILMITopoc.log, NMServer.log, and fileTopoc.log
- nmControl.dump
- CMSCclient.log

Possible alternative workaround—Open a new GUI and a new Configuration Center, Chassis View, Diagnostics Center, or Statistics Report.

J.10.5.5.6 Transient Event Has Disappeared Unexpectedly

Transient alarms behave somewhat differently depending on whether the entity is managed by the network element or the NMS itself. If the transient alarm is on a managed network element; for example, an alarm generated by an FTP transfer failure, then the alarm is self-clearing. This means if the same transient alarm happens more than twice, the previous active alarm is cleared by the latest.

If the transient alarm is not a managed network element, but rather the NMS itself, then the alarm is not self-clearing and there will be multiple occurrences of the same alarm conditions. Since these NMS alarms (or events) that pertain to the NMS are not cleared by the NMS, NMS alarms are not correlated. They must be cleared manually by the operator. If these events are not manually cleared, the list will grow only to the value of MAX_ACTIVE_NMS_EVENTS that is specified in the NMServer.conf file. Once the list of NMS alarms reaches MAX_ACTIVE_NMS_EVENTS, NMServer will automatically clear the oldest alarms in the list to make room for the new events. The number of events that will be cleared each time the maximum is reached is also specified in NMServer.conf. That configuration parameter is called EVENTS_TO_CLEAR_WHEN_MAX_REACHED.

If there was a transient event that has unexpectedly disappeared, it is most likely because NMServer purged the event.

Step 1 Filter the alarm list on CTM alarms.

Step 2 Check the alarm count and compare it with the MAX_ACTIVE_NMS_EVENTS value in NMserver.conf. If the alarm count is close to the MAX_ACTIVE_NMS_EVENTS, then this explains why the transient event has been purged.

Step 3 If the alarm count for NMS alarms has not reached the MAX_ACTIVE_NMS_EVENTS, the missing event may have been manually cleared. The NMServer log will indicate whether the event was manually cleared.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log, NMServer.log, and CMSCclient.log
- Capture NMServer dump, use nmControl

Possible alternative workaround—Restart the Alarm List GUI.

J.10.5.5.7 Port in Tree View Displays Aggregate Alarm; However, No Children Exist Under Port

The tree view in CTM client GUIs displays network elements from the top-level physical view down to the port. Alarm severities are aggregated from children up to parents. Since the port is at the lowest level of the tree, the question that often arises is how a port can have an aggregate alarm if it has no children. The answer to this question is that connections are virtual entities under ports in the tree view. Virtually, you will not see connections in the tree. But connection alarms are aggregate up to the port in the tree view.

Step 1 Compare the connection alarms with the aggregate port alarms:

a. In the Configuration Center, click the **Connections** tab.

b. Find the port in the tree view and drag and drop it to the right window pane. The Connection view window appears.

c. Click the **Get** button. The connections should be listed, and the alarm status should match the alarm status in the alarm list.

Step 2 If the connection alarms do not match the aggregate port alarm(s) in Alarm List GUI, there may be a defect. Collect the following defect information:

- CMSCclient.log, NMServer.log, sdbroker*.log, xdbroker*.log
- Capture NMServer dump, use nmControl

Possible alternative workaround—None.

J.10.6 Chassis View Problems

This section includes the following information:

- J.10.6.1 Chassis View Basics, page J-69
- J.10.6.2 Lines Not Displayed in the Chassis View, page J-70
- J.10.6.3 Card Not Displayed in the Chassis View, page J-70
- J.10.6.4 DCA/DCB Status Not Displayed on PXM Cards, page J-71
- J.10.6.5 Ethernet Status Not Updated on PXM Cards, page J-71
- J.10.6.6 HIST, CBRX, and CBTX Status Not Updated in MGX Nodes, page J-71
- J.10.6.7 RPM Card Status Not Updated, page J-71
- J.10.6.8 RPM Secondary Card Status Is Blue, page J-71
- J.10.6.9 Lines Not Displayed on Secondary Card, page J-71
- J.10.6.10 Lines Not Selectable, page J-72
- J.10.6.11 Wrong Tooltip Is Displayed, page J-72

J.10.6.1 Chassis View Basics

Chassis View is a read-only application that provides the physical view of WAN devices. For a specific node, it displays node, cards, and lines. Chassis View does not display ports. It can handle the following events:

- Node status changes
- Card status changes
- Line status changes

The alarms handled by Chassis View are:

- Card alarm
- Line alarm

Chassis View shows an empty slot in the chassis when displaying unsupported cards. For a reserved card, it shows the lines, but they are disabled. Chassis View does not show lines under a card when the card is in another state, other than active or standby.

Chassis View displays the chassis by combining static data from the XML file and dynamic data from the database. The first step in debugging is to determine if data is populated properly in the database. The next step is to check that the card or line is defined in the XML file.

J.10.6.2 Lines Not Displayed in the Chassis View

Step 1 Determine if data about the lines are populated for the corresponding lines in the line table in the database.

Step 2 Check whether the lines are defined in the XML file Chassis View.xml.

Step 3 Make sure that the line numbers in the database start from 1 and not from 2 or above.

Step 4 Make sure that the node is in sync (mode is 3).

If the details are not found in the database, this probably is an EM issue. If the details are found, then proceed as follows:

a. Use **cwmver** to get the CTM version.

b. Get the node table information for the node using the following command; then, save it in a file:

```
echo "select (*) from the node, where node_id=<NodeId> " | dbaccess
```

c. Get the card table information for the card using the following command; then, save it in a file:

```
echo "select (*) from the card, where node_id=<NodeId> and slot=<Slot>" | dbaccess
```

d. Save the line table information for the line using the following command:

```
echo "select (*) from the line, where node_id=<NodeId> and slot=<Slot>" | dbaccess
```

e. Save the log as CMSCclient.log to your local drive.

f. Take a copy of the chassisview.jar from the /opt/svplus/java/jars/cwm/ directory. You need to check that gif files used to draw the lines are available in the jar.

Possible alternative workaround—Select the lines from the tree view to launch other applications.

J.10.6.3 Card Not Displayed in the Chassis View

Step 1 Check that entries for the card are available in the card table.

Step 2 Check whether the lines are defined in the XML file ChassisView.xml.

Step 3 Make sure that the node is in sync (mode is 3).

If the details are not found in the database, this probably is an EM issue. If the details are found, then proceed as follows:

a. Use **cwmver** to get the CTM version.

b. Get the node table information for the node using the following command; then, save it in a file:

```
echo "select (*) from the node, where node_id=<NodeId> " | dbaccess
```

c. Get the card table information for the card using the following command; then, save it in a file:

```
echo "select (*) from the card, where node_id=<NodeId> and slot=<Slot>" | dbaccess
```

d. Save the log as CMSCclient.log to your local drive.

e. Take a copy of the chassisview.jar from the /opt/svplus/java/jars/cwm/ directory. You need to check that gif files used to draw the lines are available in the jar.

Possible alternative workaround—Select the cards from the tree view to launch other applications.

J.10.6.4 DCA/DCB Status Not Displayed on PXM Cards

DCA/DCB status is always grayed out in Chassis View. DCA/DCB status information is not received from the switch, so the status is not displayed or updated.

J.10.6.5 Ethernet Status Not Updated on PXM Cards

Ethernet status is received only when the Chassis View is launched. Dynamic changes in states of the Ethernet status are not updated in Chassis View.

J.10.6.6 HIST, CBRX, and CBTX Status Not Updated in MGX Nodes

For MGX nodes, only CPUOK LED status is updated in Chassis View. Chassis View does not manage the LEDs for HIST, CBRX, or CBTX.

J.10.6.7 RPM Card Status Not Updated

Dynamic event updates are not generated for RPM cards on MGX PXM1-based nodes, so the Chassis View does not get event updates on hot insertion or removal of RPM cards. The card will be identified when coldstart is done.

J.10.6.8 RPM Secondary Card Status Is Blue

For RPM cards, the standby state shows the card status in blue because the card has only one LED (CPUOK) to show the status of the card, unlike the other cards. For other types of cards, the standby state is indicated by a yellow LED.

J.10.6.9 Lines Not Displayed on Secondary Card

If two cards are in a redundancy relationship, the primary card (for example, the logical slot) is used to display the children and for all provisioning and troubleshooting activities, even if the primary slot becomes a standby. The secondary slot does not show any children under it, even if it becomes active. Hierarchical views in all applications behave in this manner. Similarly, provisioning is allowed only on the working line of an APS pair regardless of whether or not that line is currently active. However, monitoring is done on both working and protection lines.

J.10.6.10 Lines Not Selectable

Sometimes lines become unselectable. For example, when trying to select line 3, line 1 may get selected or vice versa.

Lines must be spaced sufficiently apart. If they are not, they may overlap, causing them to become unselectable.

Defect Information—Collect the following information for further analysis:

- Get the copy of the ChassisView.xml file used.
- Take a copy of the chassisview.jar from the /opt/svplus/java/jars/cwm/ directory. Verify that gif files were used to draw the lines.

Possible alternative workaround—Try selecting from the tree view.

J.10.6.11 Wrong Tooltip Is Displayed

When you move the cursor over a line, the wrong tooltip is displayed. For example, when moving the cursor below the last line in the card, the tooltip of the line gets displayed instead of the tooltip of the card.

Lines must be spaced sufficiently apart. If they are not, they may overlap, causing the wrong tooltip to be displayed.

Defect Information—Collect the following information for further analysis:

- Get the copy of the XML file used: ChassisView.xml for MGX nodes and BPXIGX.xml for BPX/IGX nodes.
- Take a copy of the chassisview.jar from the /opt/svplus/java/jars/cwm/ directory. Verify that gif files were used to draw the lines.

Possible alternative workaround—Try selecting from the tree view.

J.10.7 Configuration Center Management

The Configuration Center management functions are divided into the following categories:

- Network elements—Manages the nodes and their components. For network element management, the Configuration Center communicates with the Config Server process.
- Connections—Manages the connections between the nodes. For connection management, the Configuration Center communicates with the Connection Management (CM) Server process.

This section describes troubleshooting guidelines for the element management (Configuration Center; Elements Tab) section. The Connection Management (Configuration Center; Connections Tab) section describes troubleshooting guidelines related to Connection Management.

This section includes the following information:

- J.10.7.1 Configuration Center Framework, page J-72
- J.10.7.2 Configuration Center—Element Management, page J-78

J.10.7.1 Configuration Center Framework

The Configuration Center uses the CTM framework and workflow mechanism to launch applications and drag and drop objects across application.

- Network elements can be selected in the tree view and the Configuration Center (Elements Tab) can be launched to view or modify the selected object.
- Network elements can be dragged and dropped from other application to the Configuration Center's Elements tab for modification.

This section includes the following information:

- J.10.7.1.1 Cannot Launch the Configuration Center, page J-73
- J.10.7.1.2 Cannot Launch Other Applications from the Configuration Center, page J-73
- J.10.7.1.3 An Exception Is Raised when the Configuration Center Is Launched, page J-74
- J.10.7.1.4 An Exception Is Raised when the Configuration Center Launches Another Application, page J-74
- J.10.7.1.5 Element Tab—Internal Frame Does Not Launch, page J-75
- J.10.7.1.6 Element Tab—Drag-and-Drop Functionality Does Not Launch An Internal Frame, page J-75
- J.10.7.1.7 Element Tab—Create, Details, Modify, and Refresh Button Issues, page J-75
- J.10.7.1.8 Element Management—Drag and Drop Within Configuration Center, page J-75
- J.10.7.1.9 Cross Application—Configuration Center as Drag Source, page J-76
- J.10.7.1.10 Cross Application—Configuration Center’s Element Tab as Drop Target, page J-76
- J.10.7.1.11 Element Tab—Internal Frame Displays Incorrect Object or Object Data, page J-77
- J.10.7.1.12 Configuration Center's Element Tab Does Not Respond (GUI Is Grayed Out), page J-77

J.10.7.1.1 Cannot Launch the Configuration Center

The Configuration Center cannot be launched using one of the following methods:

- Click the **Configuration Center** icon from the Launch Center or from any application.
- Choose **Tools > Configuration Center** from any application.
- Right-click the selected node from the hierarchical tree, and choose **Configuration Center**.

Step 1 Check the configcenter.jar file. Make sure that the configcenter.jar file is located in the /opt/svplus/java/jars/cwm directory of the target machine.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.2 Cannot Launch Other Applications from the Configuration Center

The Configuration Center does not launch other applications using one of the following methods:

- Choose an application from the **Tools** menu item.
- Right-click on the selected object from the hierarchical tree and choose the target application.

Step 1 Check the target application jar file. Make sure the target application jar file is located in the /opt/svplus/java/jars/cwm directory of the target machine.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.3 An Exception Is Raised when the Configuration Center Is Launched

When the Configuration Center is launched using one of the following methods, an exception is raised and the Java Console shows the exception trace information:

- Choose an application from the **Tools** menu item.
- Right-click on the selected object from the hierarchical tree and choose the target application.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.4 An Exception Is Raised when the Configuration Center Launches Another Application

When the Configuration Center launches another application, using one of the following methods, an exception is raised and the Java Console shows the exception trace information:

- Choose an application from the **Tools** menu item.
- Right-click on the selected object from the hierarchical tree and choose the target application.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.5 Element Tab—Internal Frame Does Not Launch

When the Element tab is selected and you double-click on a supported network element, an internal frame is not created or the content of an existing internal frame is not recycled.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.6 Element Tab—Drag-and-Drop Functionality Does Not Launch An Internal Frame

When the Element tab is selected and you drag and drop supported network elements to the Element tab's content pane, an internal frame is not created or the content of an existing internal frame is not recycled.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.7 Element Tab—Create, Details, Modify, and Refresh Button Issues

When the Element tab is selected and an object is displayed in an internal frame, the Create, Details, Modify, and Refresh buttons either do not launch other internal frames for further provisioning or they do not update the user interface with data for the selected operation.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.8 Element Management—Drag and Drop Within Configuration Center

The drag-and-drop functionality of a network element from the Configuration Center tree view to the Element tab's content pane does one of the following:

- Fails to open an internal frame
- Fails to recycle the contents of an existing frame to display the object's attributes

- Results in the Operation Not Supported message box

Step 1 Determine if the drag-and-drop functionality is supported for the dropped object.

The following objects can be dropped from the tree view to the content pane:

- For the Element tab, the Network, Node, Card, Line, Port, IMA, and IMA link objects are supported and Folder objects are not supported.
- For the Connection tab, the Node, Card, Line, and Port objects are supported and Folder, IMA, and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information, specifically any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.9 Cross Application—Configuration Center as Drag Source

As drag source, the drag-and-drop functionality of an object from the Configuration Center's tree view or Element tab to another CTM application fails to display the selected object in the target application.

Step 1 Determine if the drag-and-drop functionality is supported for the selected object.

Step 2 Determine if the target application supports the drag-and-drop functionality for the dropped object.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information, specifically any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.10 Cross Application—Configuration Center's Element Tab as Drop Target

The drag-and-drop functionality of a network element from another CTM application to the Configuration Center's Element tab content pane does one of the following:

- Fails to open an internal frame
- Fails to recycle the contents of an existing frame to display the dropped object's attributes
- Results in the Operation Not Supported message dialog box

Step 1 Determine if the drag-and-drop functionality is supported for the dropped object.

The following objects can be dropped from the tree view to the content pane:

- For the Element tab, the Network, Node, Card, Line, Port, IMA, and IMA link objects are supported and Folder objects are not supported.
- For the Connection tab, the Node, Card, Line, and Port objects are supported and Folder, IMA and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information, specifically any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.11 Element Tab—Internal Frame Displays Incorrect Object or Object Data

The Element tab successfully creates the internal frame but either it displays information related to another object or the object's attribute values are not valid.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information, specifically any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.1.12 Configuration Center's Element Tab Does Not Respond (GUI Is Grayed Out)

The Configuration Center's Element tab does not respond and the GUI is grayed out.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file from the /opt/svplus/log directory.
- Configserver.log file from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.7.2 Configuration Center—Element Management

The Configuration Center can be used to configure different network element objects. The Configuration Center's Element tab is the main window for creating, modifying, and viewing network elements. The Element tab uses the CTM Internal Frame mechanism to display the attributes (groups and categories) associated with a particular network element. The following sections describe guidelines for troubleshooting issues related to creating, modifying, and viewing network elements.

J.10.7.2.1 XML Parsing Error

XML parsing error is seen while launching the Configuration Center (either by the drag-and-drop method or the right-click method) for a network element. The popup window says:

Internal Error: XML Parsing Error.

Step 1 Verify whether the network element, on which you want to launch the Configuration Center, is supported in the CTM version being used. If this error is seen for a supported node/card go to step 2.

Step 2 Open the /opt/svplus/log/configserver.log file and look for the message information showing when this error occurred. A typical message in the log looks like the following:

```
ERR: Fatal Error at file, line 0, char 0, Message: An exception occurred!
Type:RuntimeException, Message:The primary document entity could not be opened.
Id=/opt/svplus/xml/configcenter/XXX/XXX-XXX.xml
( <someNumber>: <x>) <someTime Stamp> ERR: InternalError: XML Parsing Error
```

If the .xml filename mentioned above has two consecutive hyphens (for example: ABC--XYZ.xml) or if it has a preceding hyphen (for example: -ABC.xml) or terminates with hyphen before the file extension (for example: ABC-.xml) proceed to step 4.

Step 3 See if the .xml file mentioned in the log message exists. If it does not exist, contact CTM engineers.

Step 4 Perform the following substeps to investigate incorrectly formed XML filename strings. The format of XML filenames is <Platform>-<Card>-<InterfaceType>-<SomeEntityName>.xml. This format is generic with a few exceptions. Also note that Platform and InterfaceType are optional and will not be seen in many files. For example, ABC-Card.xml is a valid XML filename.

a. If the Platform part of the XML filename is incorrect/missing, check the Node table to see if it is correctly populated.

b. If the Card part of the XML filename is incorrect/missing, check the Card table to verify if it is correctly populated.

c. If the Interface Type part of the XML filename is incorrect/missing, check the appropriate table to verify if it is correctly populated. This table generally corresponds to the Line or Port table of the card for which this error occurred.

d. If the Entity Name part of the XML filename is incorrect, contact CTM engineers, with the defect information required.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- /opt/svplus/log/configserver.log.

- Dspcd command output from the switch for the controller card and the service module where this error is detected.
- Ddspln or dspport command output, if this error seen for a line or port.

Possible alternative workaround—None.

J.10.7.2.2 SNMP No Data Error

An SNMP NO DATA error is seen while launching the Configuration Center (either by the drag-and-drop method or the right-click method) for a network element.

See if the network element for which this error occurred is active, and that the node is synced up. To do this, use the **selnd** command on the CTM machine.

Check whether the correct community strings are used. If this error is noticed for a properly synced up node on an active element, perform the following:

Step 1 Use an SNMP Manager tool to determine whether the switch is responding to SNMP queries.

The SNMP MIB objects to be queried for a particular dialog box can be obtained from the /svplus/log/configserver.log file. Refer to the entries in this log file when this error occurs and perform the following:

a. Using HP-OV SNMP operations, perform a walk (on "system" MIB table for this example, using public community string) as /opt/OV/bin/snmpwalk -c public nodeName system.

b. If an error is seen during the SNMP operations (from the SNMP manager tool), check the switch to verify if this information should really be present. If yes, proceed to step 2.

Step 2 Collect the information from the /svplus/log/configserver.log file when this error occurs. Perform the following:

a. From the configserver.log file, identify the MIB objects that caused the error.

b. Identify the MIB to which these objects belong.

c. Verify whether these MIB objects are supported in this release. If the objects are supported, but still the SNMP agent is not responding for SNMP queries, contact CTM engineers.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots for the investigative commands used for debugging this issue.
- Configserver.log.
- Related information on the switch.

Possible alternative workaround—None.

J.10.7.2.3 Details, Create, Delete, and Refresh Buttons Are Not Enabled

The Details, Create, Delete, and Refresh buttons are enabled or disabled based on the requirement in the tabular view. These buttons are disabled when a corresponding operation is not supported.

Step 1 Open the /opt/svplus/log/configserver.log file for the MIB.

Step 2 If the Create button is disabled, use any SNMP tool to create the object using the SNMP SET operation.

- If the SNMP SET operation passes, contact CTM engineers.

- If the SNMP SET operation fails, SSH or Telnet to the CLI and try to add the element. If the operation succeeds, contact CTM engineers.

Step 3 If the Delete button is disabled, use any SNMP tool to delete the object using the SNMP SET operation.

- If the SNMP SET operation passes, contact CTM engineers.
- If the SNMP SET operation fails, SSH or Telnet to CLI and try to delete the element. If the operation succeeds, contact CTM engineers.

Step 4 The only reason why a Details button is disabled is that all the information related to the element is already displayed in the tabular view. Check the configserver.log file to determine if any MIB entry appropriate to the element is available. If a MIB entry is available, perform an SNMP walk on the MIB entry using any SNMP tool. If there are is information in addition to what is displayed in the tabular view, and if it is important to be displayed in the frame, contact CTM engineers.

Step 5 The only reason why a Refresh button is disabled is that all the information displayed in the frame is read-only. If there are any editable fields and the Refresh button is disabled, contact CTM engineers.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots for the investigative commands used for debugging this issue.
- Configserver.log

Possible alternative workaround—For creating or deleting elements, use either the SNMP SET operation on the CTM machine or CLI commands on the switch.

J.10.7.2.4 SNMP Timeout Error

This error occurs when you try to set or get values to or from SNMPCOMM and the values look like the following:

```
Check the sync-up, link0, link1 status of the Node in the inspectorview.
```

Step 1 If the status is Unmanaged, Unreachable, Failed in Sync, or Partially Synced, check the connectivity of the node using the **ping** command, Telnet, or any other utility.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots for the investigative commands used for debugging this issue.
- Configserver.log

Possible alternative workaround—None.

J.10.7.2.5 SNMP Set Error

This error occurs when the SNMP SET operation is done on an uneditable MIB object or when you use invalid values.

Step 1 Open the /opt/svplus/log/configserver.log file.

Step 2 Check for the last part of the document name.

For example, if the document name is AAA-BBB-CCC.xml, then the document AAA-BBB-CCC.xml can be found in the /opt/svplus/xml/configcenter/CCC/ directory.

Step 3 If the file is not available, contact CTM engineers.

Step 4 Open the document you got in step 2 and do the following:

- Check the Access field of the MIB object in the XML file.
- Check the Access field in the /opt/svplus/mibs directory.

If the access field from XML file and MIB definition are not same, contact CTM engineers.

Step 5 Check the Range field of the MIB object in the XML file and MIB definition. If they are not the same, contact CTM engineers.

Step 6 Perform an SNMP SET operation on the MIB object with the same value shown in the GUI and appropriate community string (as displayed in /opt/svplus/log/configserver.log) using HP-OV. A syntax of the SNMP SET operation is shown as follows:

```
/opt/OV/bin/snmpset -c private nodeName MIBVariable MIBDataType MIBValue
```

Step 7 If the SNMP SET operation succeeds, contact CTM engineers with appropriate defect information.

Step 8 SSH or Telnet to the switch and try to configure the same parameter with the value given in the GUI and SNMP tool. If the CLI does not report errors, contact CTM engineers with defect information.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots for the investigative commands used for debugging this issue.
- Configserver.log

Possible alternative workaround—None.

J.10.7.2.6 Object Not Found In Tree View Error

This error occurs when a network element is launched from the tabular view of the Configuration Center.

Step 1 Collect the information of the object being launched. This can be done in two ways.

- In the tabular view, there will be some minimal information such as node name, slot number, line number, trunk number, port number, and so on.
- Some minimal information regarding the object being launched will be displayed in the title of the window in one of the following formats:
  - For a node, the window title will have <NodeName>
  - For a slot, the window title will have <NodeName>.<SlotNumber>
  - For a line, the window title will have <NodeName>.<SlotNumber>.<LineNumber>
  - For a port, the window title will have <NodeName>.<SlotNumber>.<PortNumber>

Step 2 With the information obtained from Step 1, see if that object appears in the tree view.

- If it does appear, go to step 3.
- If it doesn't appear, refresh the tabular view two or three times and see if the object still exists in the tabular view, and if it continues giving the same error, contact CTM engineers with the appropriate defect information.

Step 3 If the object being launched is a node or card, verify whether that particular node or card is supported in the CTM version being used.

Step 4 If the node or card is supported, open the /opt/svplus/log/CMSCclient.log file and check whether the FDN of the object being launched matches the information from Step 1. Contact CTM engineers with appropriate defect information. A typical example of the log follows:

```
[DD Mon YYYY HH:MM:SS] DEBUG - [appsConfigCenter] :: CcElementInternalFrame :
modifyActionPerformed()
[DD Mon YYYY HH:MM:SS] DEBUG - [appsConfigCenter] CcTabularView : modify()
[DD Mon YYYY HH:MM:SS] INFO - [appsConfigCenter] Selected fdn =
/NW=X/RND=XX/CD=X/LN=X/PT=X
```

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>og directory.
- Java Console information.
- Contents of /opt/svplus/log/configserver.log file.

Possible alternative workaround—None.

J.10.7.2.7 Element Data Inconsistent with Switch

Information displayed in the GUI and the switch is not the same.

Step 1 Make sure that the window has been launched for the correct element in the GUI. If not, contact CTM engineers with the defect information.

Step 2 SSH or Telnet to the switch, change a few parameters, and see if the change is reflected in the GUI. If not, contact CTM engineers.

Step 3 Open the /opt/svplus/log/configserver.log file and find the MIB OID of the element that displays the inconsistent data.

Step 4 See if the MIB OID is pointing to the information that you are looking for. If not, contact CTM engineers.

Step 5 Use any SNMP tool to perform an SNMP GET operation on the MIB object which shows inconsistent. If the value retrieved using the SNMP GET operation and the value shown in the GUI are not the same, contact CTM engineers. The following shows the syntax of the SNMP GET operation in a HP-OV:

snmpget [-Cf] [options...] <hostname> {<community>} [<objectID> ...]

Step 6 Check the data type of the MIB object that shows inconsistent data. If the data type of the MIB object in the configserver.log is not the same as the data type defined in the MIB object definition (available at /opt/svplus/mibs/ directory), contact CTM engineers with defect information.

Step 7 Check the data type of the MIB object:

a. If the data type of the MIB object is Bitmap, then convert the decimal value of the MIB object to a binary value and compare the bits SET/RESET with the values defined in the MIB object definition and displayed in the GUI. Contact CTM engineers with defect information.

b. If the data type of the MIB object is an IpAddress, verify whether the value is in the appropriate format, for example, <aaa.bbb.ccc.ddd>. If the value is not in proper format, contact CTM engineers.

Defect Information—Collect the following information for further analysis:

- Screen snapshots for the investigative commands used for debugging this issue

- /opt/svplus/log/configserver.log

Possible alternative workaround—None.

J.10.7.2.8 Config Server Reports Error Messages

This section describes the various kinds of errors that could happen on the config server.

Step 1 Open the /opt/svplus/log/configserver.log file.

Step 2 If data type mismatch occurs, an error message is displayed in the GUI and the corresponding error message seen in configserver.log file is as follows:

```
( 24560: 9) 07:49:14 CRIT: %SnmpCommException-2-NOT_INTEGER_VALUE:
SnmpVar::getInteverValue() incorrectly called for ASN type [4].
```

In this case, the data type of the MIB object defined in the XML file is not the same as the data type of the MIB object definition. Contact CTM engineers with defect information.

Step 3 If you enter an invalid value, an error message is displayed in the GUI with the parameter name appended. The corresponding error message seen in configserver.log file is as follows:

```
( 17252: 6) 08:31:20 ERR: %SnmpCommException-3-ERR_BADVALUE: Snmp Error[3]: Bad Value;
object [] (index[2]) :
```

Step 4 If you try to up/add more than one element, an error message is thrown in the GUI and the corresponding error message thrown in the /opt/svplus/log/configserver.log file is as follows:

```
( 23868: 6) 14:01:09 ERR: %SnmpCommException-3-ERR_GENERR: Snmp Error[5]: General Error;
object [] (index[0])
```

Defect Information—Collect the following information for further analysis:

- Collect all complete screen snapshots for the investigative commands used for debugging this issue.
- Contents of /opt/svplus/log/CMSCclient.log file.

Possible alternative workaround—None.

J.10.8 Connection Management Problems

This section includes the following information:

- J.10.8.1 Configuration Center GUI—Framework Issues, page J-83
- J.10.8.2 Configuration Center GUI—CM Server-Reported Errors, page J-87
- J.10.8.3 Cmsvr Errors, page J-90
- J.10.8.4 CMGRD, page J-95

J.10.8.1 Configuration Center GUI—Framework Issues

The Configuration Center management functions are divided into the following categories:

- Connections—Manages the connections.

Note For connection management, the Configuration Center communicates with the Connection Management Server process.

- NE—Manages the nodes and their components.

Note For network element management, the Configuration Center communicates with the Config Server process.

The Configuration Center's Connection tab is the main window for creating, modifying, and viewing network connections. The Connection tab content pane provides additional tabs for creating connections (Advanced Mode and Quick Mode tabs) and retrieving a list of existing connections (Connection tab).

The Configuration Center uses the CTM framework and workflow mechanism to launch applications and to create and display connection information.

- Connections can be selected in CTM applications, and the Configuration Center (Connection Tab) can be launched to view/modify the selected connection.
- Connections can be dragged and dropped from other application to the Configuration Center's Connection tab for modification.

The following sections describe guidelines for troubleshooting issues related to creating, modifying, and viewing network connection using the Configuration Center.

J.10.8.1.1 Connections Tab—Double-Click Operation on Tree View Does Not Launch Connection's Internal Frame

The double-click operation on a network element in the tree view on the Connection tab (a) fails to open an internal frame, (b) fails to recycle the contents of an existing internal frame to display the double-clicked connections attributes, or (c) results in the Operation Not Supported message dialog box.

Step 1 Determine if the double-click operation is supported for the selected object.

The Connection tab supports connection management for the Node, Card, Line, and Port objects. The drag-and-drop functionality of Folder, IMA, and IMA link objects is not supported.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file from the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.2 Connections Tab—Drag and Drop Does Not Launch Connection's Internal Frame

The drag-and-drop functionality of a network element from the Configuration Center tree view to the Connections tab's content pane (a) fails to open an internal frame, (b) fails to recycle the contents of an existing frame to display the dropped object's attributes, or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine if the drag-and-drop functionality is supported for the dropped object.

The Connection tab supports the drag-and-drop functionality for the Node, Card, Line, and Port objects. The drag-and-drop functionality of Folder, IMA, and IMA link objects is not supported.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.3 Connection List Tab—Cannot Launch Internal Frame to Modify an Existing Connection

The Details button fails to launch an internal frame to display the connection details for a retrieved connection.

Step 1 Check that the connection status is not in the Incomplete state.

Only connection in the OK and Fail states can be launched using the Details button on the Connection tab.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.4 Advanced Mode Tab—Cannot Launch the Connection Details Dialog Box Using the Details Button

The Details button on the Advanced Mode tab fails to launch the Connection Details dialog box.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.5 Advanced Mode Tab—Cannot Launch the Template Details Dialog Box Using the Template Details Button

The Template Details button on the Advanced Mode tab fails to launch the Template Configuration dialog box.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.6 Cross Application—Cannot Launch Other Applications from the Connection List

For a retrieved connection on the Connection tab, the right-click popup menu does not launch the selected target application for the connection or it results in the Operation Not Supported message dialog box.

Step 1 Determine if the operation is supported by the target application.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.7 Cross Application—Connection List as Drag Source

As drag source, the drag-and-drop functionality of a connection from the Configuration Center's connection list to another application fails to display the selected connection in the target application.

Step 1 Determine if the target application supports connection object drop operations.

Step 2 Determine if the target application supports the drag-and-drop functionality for connection objects.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.

- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.8 Cross Application—Connection Tab's Content Pane as Drop Target

The drag-and-drop functionality of a connection object from another application to the Configuration Center's connection tab content pane (a) fails to open an internal frame, (b) fails to recycle the contents of an existing frame to display the newly dropped connection object, or (c) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine if the source and the target application belong to the same instance of the Java virtual machine (VM). CTM framework does not support drag-and-drop functionality across applications belonging to different Java VMs.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.1.9 Configuration Center's Connection Tab Does Not Respond

The Configuration Center's Connection tab does not respond and the GUI is disabled.

Step 1 Try to reproduce the problem in order to collect additional Java-related data using the Java DOS window.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.2 Configuration Center GUI—CM Server-Reported Errors

For connection management, the Configuration Center communicates with the Connection Management (CM) Server process to (a) create, modify, delete, or retrieve connections and (b) create, modify, delete, or retrieve a connection template. The CM Server throws application exceptions if it cannot successfully complete the requested operation. The CM Server exception contains an error message that describes the error condition. The Configuration Center displays the reported error message for further analysis. In

such cases, the problem must be researched on the CM Server side. The CM Server troubleshooting sections describe the steps required to further analyze the CM Server-related issues. See J.10.8 Connection Management Problems, page J-83. In this section, the required validation and data collection procedures related to the Configuration Center are presented.

J.10.8.2.1 Connection Creation, Modification, Deletion, and Retrieval Errors

When performing any connection creation, modification, deletion, and retrieval, the CM Server could encounter an error and notify the Configuration Center by throwing an application exception error that contains information describing the error. As a result, the Configuration Center displays the error message. The following lists some CM Server-related exceptions.

```
DATABASE_ERROR:"Database error [%s]."
UNKNOWN_EXCEPTION: "Program Error. Unknown Exception is caught in [%s]."
SUBSYSTEM_EXCEPTION:"Program Error. Subsystem exception [%s] caught in [%s]"
INTERNAL_ERROR: "Program or System Error. Function [%s] reports: [%s]"
CONNECTION_LOST: "Connection from host [%s] application [%s] lost during request."
UNKNOWN_PARAM_VALUE_TYPE: "Unknown parameter value type [%d] is processed in [%s]."
PARAM_TYPE_VALUE_MISMATCH: "Parameter value [%s] is does not match type [%d]"
VALUE_OUT_OF_RANGE: "Value [%d] is outside of the valid [%d] - [%d] range"
NO_SUCH_CONNECTION_TYPE_ENUM: "No such connection type enum [%d]"
NO_SUCH_SERVICE_TYPE_ENUM: "No such service type enum [%d]"
NO_SUCH_ENDPOINT_TYPE_ENUM: "No such endpoint type enum [%d]"
NO_PORT_TABLE_INFO_FOR_CARD: "No port table information for card family [%d]"
NO_LINE_TABLE_INFO_FOR_CARD: "No line table information for card family [%d]"
FILTER_REQUIRED:"Filter [%s] is required"
UNEXPECTED_PARAMSET: "CM Server does not expect parameter set [%d]."
UNSUPPORTED_ENDPOINT: "CM Server does not support end point with card type [%s], vs[%s],
interface type [%s], node platform [%s], controller type [%s] for connection type [%s]
service type [%s], endtoend type [%s]."
UNSUPPORTED_PARAMETER_FOR_VISM: "Unsupported parameter setting on the [%s] end. CM Server
does not support [%s] + [%s] PVC's for VISM cards with firmware revision less than [%s]
and card mode set to [%s]."
PROTECTED_CONNECTION: "[%s] end of the connection is protected. Protected connections
cannot be deleted."
UNSUPPORTED_NODE_PLATFORM: "CM Server does not support node platform [%d]."
UNSUPPORTED_CONN_TYPE: "CM Server does not support Connection of type [%d]."
UNSUPPORTED_SERV_TYPE: "CM Server does not support Connection type [%s] , Service type
[%s] and Endtoend type [%s] between Card type [%s] and [%s]."
UNSUPPORTED_SERV_TYPE_ONE_END: "CM Server does not support Connection type [%s] , Service
type [%s] and Endtoend type [%s] on Card type [%s]."
UNSUPPORTED_CARD_PAIR: "Connection between card type [%s] and card type [%s] is not
supported."
NO_SUCH_NODE_ID_IN_DB: "Node id [%d] not found in table [node]."
NO_SUCH_NODE_NAME_IN_DB: "Node name [%s] not found in table [node]."
NO_SUCH_CARD_IN_DB: "Card : Node[%d], Slot[%d] not found in table [card]."
NO_SUCH_LOG_PORT_IN_DB: "Card : Node[%d], Slot[%d], LogPort[%d] (%d - in database), not
found in table [%s]."
NO_SUCH_PHY_PORT_IN_DB: "Card : Node[%d], Slot[%d], Line[%d], PhyPort[%d] (%d - in
database), not found in table [%s]."
NO_SUCH_LINE_IN_DB: "Card : Node[%d], Slot[%d], Line[%d] not found in table [%s]."
NO_SUCH_CONNECTION_IN_DB: "Connection [%s] not found in database"
UP_CONN_FAILED: "Upping Connection Failed. Test Result from switch [%s]"
DOWN_CONN_FAILED: "Downing Connection Failed. Test Result from switch [%s]"
NO_ONE_SEGMENT_HYBRID: "Cannot create one segment hybrid connection."
INCORRECT_LINE_SUBTYPE: "Incorrect Line SubType. Line: Node[%d],slot[%d],ifindex[%d] is
[%d] not [%d]."
INVALID_LINE_NUMBER: "func [%s]:Invalid Line Number(s)."
NO_CONTROLLER_IN_PORT: "node[%s] slot[%d] port[%d] does not have controller of type [%s]";
INVALID_FDN: "The given FDN format or value is invalid. [%s]"
INVALID_PORT: "Provisioning operations are not allowed on feeder trunk/routing trunk and
XLMI trunk ports. [%s]"
```

Step 1 Verify that the CM Server and sdbroker are up and running by entering **psg sdbroker** and **psg cmserver** on the command line.

Step 2 Verify if the CmServer restarted while the operation was being done by checking the cmsvr.log and searching for the string "START OF THE PROCESS". Verify that the time stamp of the server process was restarted while the operation was being performed. Also check for any cmsvr coredumps under the /opt/svplus/corefilesdir/ directory.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.2.2 Connection Template Creation, Modification, Deletion, and Retrieval Errors

When performing any connection template creation, modification, deletion, and retrieval, the CM Server could encounter an error and notify the Configuration Center by throwing an application exception error that contains information describing the error. As a result, the Configuration Center displays the error message. The following lists some CM Server-related connection template exceptions:

- CONN_TEMPLATE_ALREADY_PRESENT: "The Connection Template[%s] is already present in the conn_template table."
- CONN_TEMPLATE_NOT_PRESENT: "The Connection Template[%s] is not present in the conn_template table."
- CONN_TEMPLATE_TABLE_INCONSISTENT: "The Connection Template table contains more than one entry for the template[%s]."
- CONN_TEMPLATE_PARAMS_NOT_PRESENT: "The Connection Template[%s] is not present in the conn_templ_param table."
- DATABASE_ERROR:"Database error [%s]."
- UNKNOWN_EXCEPTION: "Program Error. Unknown Exception is caught in [%s]."
- SUBSYSTEM_EXCEPTION: "Program Error. Subsystem exception [%s] caught in [%s]."
- INTERNAL_ERROR: "Program or System Error. Function [%s] reports: [%s]."

Step 1 Verify that the CM Server, sdbroker, and xdbroker are up and running by entering **psg sdbroker**, **psg xdbroker**, and **psg cmserver** on the command line.

Step 2 Verify if the CM Server restarted while the operation was being done by checking the cmsvr.log and searching for the string "START OF THE PROCESS". Verify that the time stamp of the server process was restarted while the operation was being performed. Also check for any cmsvr coredumps under the /opt/svplus/corefilesdir/ directory.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information; in particular, any Java-raised exceptions.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- Configserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.3 Cmsvr Errors

The following are some of the most common errors seen when a provisioning request is issued:

- J.10.8.3.1 End-to-End Type Cannot Be PVC for Connections with PNNI Segment, page J-90
- J.10.8.3.2 Unsupported Service Type for the Foresight Connections for PNNI/SPVC Endpoints, page J-91
- J.10.8.3.3 CE-CE Connection Port Speed Should Be the Same on Both Endpoints, page J-91
- J.10.8.3.4 Cannot Create One-Segment Hybrid, page J-91
- J.10.8.3.5 Cannot Add Connection Between -byte Port Header and -byte Port Header for chan type NIW and NIW-replace, page J-91
- J.10.8.3.6 Unsupported Service Type—General node-slot-port-version, page J-92
- J.10.8.3.7 Endpoint Is Not Present in One of the Connection Tables During a Modify Operation, page J-92
- J.10.8.3.8 Cmsvr—Connection Diagnostic Issues, page J-93
- J.10.8.3.9 TestConn or TestDelay Failed with Switch Error, page J-93
- J.10.8.3.10 Connection Up/Down/Reroute Failed, page J-94
- J.10.8.3.11 Connection Trace Failures, page J-94

J.10.8.3.1 End-to-End Type Cannot Be PVC for Connections with PNNI Segment

When an add connection is attempted, cmsvr checks its the endpoints and the end-to-end type to make sure it is supported. The error message states "EndtoEndType cannot be PVC for connections with a PNNI segment."

The problem must be fixed on the CM GUI while adding the connection.

Step 1 Verify that the endpoints that are being used to add the connection are not on PNNI nodes or feeders to PNNI nodes.

Step 2 Change the end-to-end type in the CM GUI to either SPVC or Hybrid.

Defect Information—Collect the cmsvr logs from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.3.2 Unsupported Service Type for the Foresight Connections for PNNI/SPVC Endpoints

During connection addition, the error message could state "CM Server does not support Connection type[], Service type[], and Endtoend type []between Card type and []." The parentheses are filled with the appropriate values.

Step 1 Determine if the service type is applicable to the endpoints.

Step 2 Determine the cards on which the connection is being added and the service type given in the GUI.

This error is thrown when the service type is either abr-fs, atfst for a PVC, SPVC or Hybrid end to end type and the card is either a pxm, axsm, rpm, or frsm12 card.

Defect Information—Collect the cmsvr logs from the /opt/svplus/log directory.

Possible alternative workaround—Change either the endpoints or the service type to add the connection.

J.10.8.3.3 CE-CE Connection Port Speed Should Be the Same on Both Endpoints

While adding a CE-CE connection, this error message might be thrown:

"For Ce-Ce Connection Port Speed should be same on both sides. Port Type should be same except for Structured 8T1 and E1."

Step 1 Make sure that the port speed is the same for both the local and remote endpoints.

Step 2 Make sure that the port types are the same for both the end types, except for structured 8T1 and 8E1.

Defect Information—Collect the cmsvr logs in the directory /opt/svplus/log.

Possible alternative workaround—Change the endpoints accordingly to add the connection.

J.10.8.3.4 Cannot Create One-Segment Hybrid

While adding a one segment connection, a check is made to make sure that it is not a hybrid connection. If it is, the following error message appears:

"Cannot create one segment hybrid connection."

Step 1 Make sure the end-to-end type is not Hybrid for a single-segment connection.

Defect Information—Collect the cmsvr logs in the directory /opt/svplus/log.

Possible alternative workaround—Change the end-to-end type to something other than Hybrid.

J.10.8.3.5 Cannot Add Connection Between -byte Port Header and -byte Port Header for chan type NIW and NIW-replace

During a connection addition between two FRSM_12 ports, the cmsvr checks to see if the port headers are the same (4-byte or 2-byte) for both the endpoints. An error is thrown if they are not:

"Cannot add Connection between 4 byte port header to 2 byte port header for chan type NIW or NIW-replace."

Step 1 Determine what port header was used while creating the port in question. Then use ports with matching port headers to create the connection.

Defect Information—Collect the cmsvr logs from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.3.6 Unsupported Service Type—General node-slot-port-version

During a connection addition, the cmsvr checks the node, slot, and port versions to ensure that the service type is supported on that version of the node, card, and port.

Step 1 Make sure that the version of the node, slot, or port supports that service type from CTM.

Step 2 Check the ConnGroupService.mib as an additional check for the versions and the supported parameters.

Defect Information—Collect the cmsvr logs from the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.8.3.7 Endpoint Is Not Present in One of the Connection Tables During a Modify Operation

When a connection modification is attempted, an error message is thrown:

"Connection [] not found in database."

Step 1 Verify that a row (entry) exists for the connection in the user_connection. Perform a query:

```
%> echo "select (*) from user_connection where l_node_id = A and l_slot = B and l_port = C
and l_subchnl_1 = D and l_subchnl_2 = E" | dbaccess stratacom
```

Step 2 If it does not exist, look in the corresponding connection table to see if the connection exists. Connection entries are as follows:

- connection for FR
- atm_connection for atm segments
- cesm_connection for cesm segments
- rpm_connection for rpm segments
- voice_conn for vism segments

Step 3 If it does not exist, look in the dbkr_temp table for an entry for that connection.

Defect Information—The following log files need to be collected:

- Cmsvr, sdbroker and corresponding em logs, in the directory /opt/svplus/log.
- Outputs of the database entries for the endpoints in the segment tables and user_connection table.

Possible alternative workaround—Resync the node or wait for sync-up to complete.

J.10.8.3.8 Cmsvr—Connection Diagnostic Issues

The cmsvr processes validates and services the connections provisioning requests from the CM GUI.

During an add, modify, or delete connection request, the request is forwarded to the cmgrd process through an ILOG (IPC) request. If the request is for connection diagnostics such as testdelay or testconn (except conntrace), cmsvr sends it to the snmpcomm process for forwarding to the switch.

J.10.8.3.9 TestConn or TestDelay Failed with Switch Error

Connection diagnostics (testdelay/testcon/up/down/reroute) fail with one of the following error messages:

- TestDelay failed with Switch error
- TestConn failed with Switch error

Step 1 Query the connection information from the user_connection table for that connection. If possible, execute the testdelay/testcon diagnostics for the same connection from ConnProxy (Service Agent) and verify the results.

Step 2 Query the connection information from the switch CLI and verify the connection status (dspcon or dspchan).

Step 3 Execute the testdelay/testcon diagnostics from the switch CLI and verify that the results match what was reported in CTM (tstdelay, tstconn).

Defect Information—Do the following:

- Capture selnd output
- Copy all the cmsvr logs from the /opt/svplus/logs directory
- User_connection table query output from the CTM database for the given endpoint (if the request is not an addition request)
- Switch CLI output for the testdelay/testconn diagnostics on the same connection

Possible alternative workaround—Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections and so on). After the connection comes up and is in the Clear state, rerun the testdelay/testconn diagnostics.

Note The testcon is not applicable for single-end SPVC connections and on AXSM card types.

Note The connection status should be Clear or Fail for the testdelay/testcon diagnostics to be executed, otherwise the test will be blocked from cmsvr.

Note The testconn/testdelay diagnostics cannot be done on RP- to-RPM connections.

Note The testdelay diagnostic is not applicable for voice and data connections.

Note For any connection, if the local end of the connection does not support that particular diagnostic, cmsvr will verify if the diagnostic can be executed from the remote end. If the diagnostic is not supported by both endpoints of a connection, an appropriate error message will be given.

J.10.8.3.10 Connection Up/Down/Reroute Failed

Connection up/down/reroute diagnostic failed with a switch error.

Step 1 Query the connection information from the user_connection table for that connection.

Step 2 Query the connection information from the switch CLI and verify the connection status (dspcon or dspchan).

Step 3 Execute the up/down/reroute diagnostic from the switch CLI and verify that the results match what was reported in CTM (upcon, dncon, rrtcon).

Defect Information—Do the following:

- Capture selnd output
- Copy all the cmsvr logs from the /opt/svplus/logs directory
- Capture the user_connection table query output from the CTM database for the given endpoint (if the request is not an addition request)
- Switch CLI output for the up/down/reroute diagnostics on the same connection

Possible alternative workaround:

a. Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections and so on). After the connection comes up and is in the Clear state, rerun the up/down/reroute diagnostics.

b. Verify the connection status to find out if the connection is already down when trying to do a down operation, or the connection is already up when trying to do an up operation.

Note The connection reroute might take the connection to the Fail state for a while.

J.10.8.3.11 Connection Trace Failures

Step 1 Make sure the connection is not in the Fail state. Connection trace does not work on failed connections; in addition, CTM does not block this request.

Step 2 Query the connection information from the user_connection table for that connection.

Step 3 Query the connection information from the switch CLI and verify the connection status (dspcon or dspchan).

Step 4 Execute the connection trace diagnostics from switch CLI and verify that the results match what was reported in CTM (conntrc, dsptrcbuffer).

Defect Information—Do the following:

- Capture selnd output
- Copy all the cmsvr logs from /opt/svplus/logs directory
- Copy all the cmgrd logs from /opt/svplus/logs directory
- Capture the user_connection table query output from the CTM database for the given endpoint (if the request is not an addition request)
- Switch CLI output for the trace diagnostics on the same connection

Possible alternative workaround:

a. Check the status of the connection and clear any alarms due to line/port issues (adding loopback, correcting the physical cable issues by verifying the physical port connections and so on). After the connection comes up and fine in the Clear state, rerun the trace diagnostics.

b. Verify the connection status. If the connection status is Down, trace cannot be executed on the connection. If the connection status is failed, the trace result will probability be an empty string.

Note The connection trace cannot be executed on an incomplete, or DAX PNNI segment connections.

J.10.8.4 CMGRD

This section includes the following information:

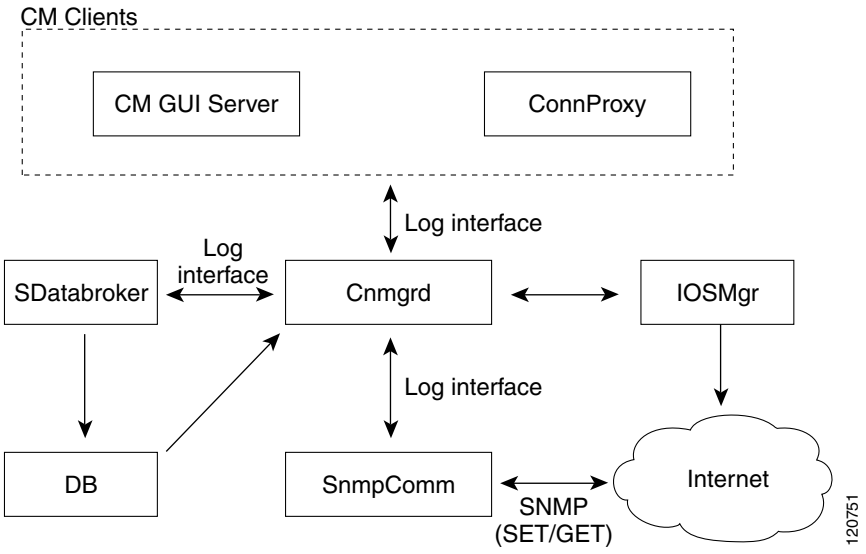
- J.10.8.4.1 High-Level Connection Management Subsystem Architecture, page J-96
- J.10.8.4.2 Cmgrd—Sdbroker Errors, page J-97
- J.10.8.4.3 Cmgrd—Sdbroker Addition/Modification/Deletion Errors: Adding a Connection Results in "Fail to Communicate with sDatabroker" Error, page J-97
- J.10.8.4.4 Cmgrd—Sdbroker Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "sDatabroker process busy. Please retry" Error, page J-97
- J.10.8.4.5 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "CTM sync-up in progress" Error, page J-98
- J.10.8.4.6 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "No more vpi/vci available for local trunk end" Error, page J-98
- J.10.8.4.7 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "EndPoint Exists Local/Remote/Both end of the connection already exists." Error, page J-99
- J.10.8.4.8 Cmgrd—Sdbroker Modification/Deletion Errors: Modifying or Deleting a Connection Results in "sDatabroker Could not lock connection entry." Error, page J-100
- J.10.8.4.9 Cmgrd Errors, page J-100
- J.10.8.4.10 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Fail due to Switch Timeout" Error, page J-100
- J.10.8.4.11 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in “Agent not responding, request timed-out; or Fatal error, Snmpcomm is not running.” Error, page J-101
- J.10.8.4.12 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Outstanding request exists for same object." Error, page J-101
- J.10.8.4.13 Cmgrd—Addition/Modification/Deletion Errors: Provisioning a Connection Results in "Fatal error, IOSMGR is not running, may need to be manually started" Error, page J-102

- J.10.8.4.14 Cmgrd—Addition Errors: Provisioning a Connection Results in "Vpi/vci ranges retrieval from svc_operation failed" Error, page J-102
- J.10.8.4.15 Cmgrd—Addition/Modification/Deletion Errors: Provisioning a Connection Results in "Can't get segment info from Data-base." Error, page J-103
- J.10.8.4.16 Cmgrd—Switch Errors, page J-103
- J.10.8.4.17 Cmgrd—Addition and Modification Errors: Provisioning a Connection Results in "Agent reported bad/wrong value for one of the variables in the request." Switch Error, page J-103
- J.10.8.4.18 Cmgrd—Addition Errors: Provisioning a Connection Results in "Object Exists on the Agent or Specified VPI/VCI not available." Switch Error, page J-104
- J.10.8.4.19 Cmgrd—Addition/Modification Errors: Provisioning a Connection Results in "Requested cell rate (lscr/lpcr or rpcr/rscr) is too high" Switch Error, page J-104
- J.10.8.4.20 Cmgrd—Addition Errors: Provisioning a Connection Results in "SPVC is not allowed on this interface" Switch Error, page J-105
- J.10.8.4.21 Cmgrd—Addition Errors: Provisioning a Connection Results in "Local Channels not enough." Switch Error, page J-105
- J.10.8.4.22 Cmgrd—Addition and Modification Errors: Provisioning a Connection Results in "Error in Traffic Parameters." Switch Error, page J-105
- J.10.8.4.23 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Network Busy, try later" Switch Error, page J-106
- J.10.8.4.24 Cmgrd—Modification Errors: Modifying a Connection Results in "Connection does not exist in CproDb/Agent returned no such name" Switch Error, page J-106

J.10.8.4.1 High-Level Connection Management Subsystem Architecture

Figure J-6 gives a high-level view of the Connection Management Subsystem.

Figure J-6 Connection Management Subsystem



Related key index entries: connproxy, cmserver, xcmgrd, cmgrd

The Connection Management Subsystem comprises the following modules:

- ConnProxy—The SNMP Agent Interface for Connection Management.
- CmServer—Provides the backend functionality to the Connection Management GUI.
- Cmgrd—The backend module, which accepts requests from ConnProxy, CmsServer Clients and issues the SNMP VarBinds to the switch for addition, modification, and deletion. Subsequently, cmgrd informs sdbroker after an addition, modification, and deletion operation of the status of the particular request, upon which sdbroker updates the CTM database.

The following errors are applicable to all types of connections: PVC, SPVC, XPVC, and hybrid.

J.10.8.4.2 Cmgrd—Sdbroker Errors

During an addition request, cmgrd could return errors that it has received from sdbroker. The following are some of the most common errors seen when a provisioning request is issued.

J.10.8.4.3 Cmgrd—Sdbroker Addition/Modification/Deletion Errors: Adding a Connection Results in "Fail to Communicate with sDatabroker" Error

Related key index entries: cmgrd, sdbroker

When any Connection Add/Mod/Del request is made, cmgrd checks its ILOG connection with the sdbroker. This error will result when cmgrd could not verify that sdbroker is available for servicing requests. In other words the ILOG connection between them is broken.

The problem must be researched on the sdbroker side.

Step 1 Verify that the sdbroker is up and running. Execute **psg sdbroker** on the command line.

Step 2 View the sdbroker log for ILOG errors. There could be multiple sdbrokers running on the machine. To check which sdbroker cmgrd talked to for that particular request, do the following:

a. vi the cmgrd.log file, and go to the end of the file. Then do a backward search for the string sdbroker. That string should indicate the number (#) of the sdbroker that cmgrd could not talk to.

b. Execute **psg sdbroker** and then check the corresponding log file of this sdbroker.

Defect Information—Collect the following:

- Stack trace of the sdbroker process pstack <pid of sdbroker>
- Sdbroker and cmgrd logs

Possible alternative workaround—None.

J.10.8.4.4 Cmgrd—Sdbroker Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "sDatabroker process busy. Please retry" Error

Related key index entries: cmgrd, sdbroker

The error message states "sDatabroker process busy. Please retry." This indicates that the cmgrd command was able to process the request and sent it to the sdbroker, but the sdbroker did not respond prior to the cmgrd's request timeout. However, between the cmgrd and sdbroker, the request appear to be working.

Defect Information:

- If the sdbroker is processing many traps (more than 20 per second) during the time of the provisioning request, then there is no sdbroker defect. Investigate the switch, NTS, or EM if you feel that there should not be so many requests occurring at the given time.
- If the sdbroker appears to be dormant, you need to capture the current status of the sdbroker. Execute the **pstack *<pid>*** command twice and save the output.

Possible alternative workaround—Repeated attempts at provisioning should be made. If there is a switch that is sending out many alarms, fixing the problem on the switch is the best solution. If the sdbroker has been 'sleeping' for a long period of time, then it should be killed and restarted.

J.10.8.4.5 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "CTM sync-up in progress" Error

Related key index entries: cmgrd, sdbroker, sync-up

While the system is in the process of syncing up, you cannot provision connections. You receive the error "CTM sync-up in progress."

You need to determine if the system is really in sync-up or not. If the system is still syncing up then this is proper operation.

Step 1 View the sync log located in /opt/svplus/log/.DBKR_SYNCHUP_MESSAGE (note the period (.) before the filename). Search for the last "xxx Start Begin at" line where xxx is either Warm or Cold. WarmStart will take a short time compared to coldstart, which could take several hours. If there is a line at the end of the file stating "Declare Sync-Up Complete" or "Warmstart Cache Rebuild Complete" then sync-up is done and there is a problem with DMD.

Step 2 If sync-up is not complete, view the start time of sync-up. Compare this to the maximum sync time identified in the /usr/user/svplus/config/dmd.conf file next to the keyword SYNCHUP_ALL_NODES_SYNC_WAIT_LIMIT. If the time taken to sync is longer than the time identified in the dmd.conf file, then DMD has a problem.

Step 3 If the system is truly still syncing up, then the system behavior is correct.

Defect Information—If there is a DMD problem, save the DMD, cmgrd, sdbroker logs, and message logs along with the .DBKR_SYNCHUP_MESSAGE and .DMD_SYNCHUP_MESSAGE* files located in the /opt/svplus/log directory.

Possible alternative workaround—Force the system to declare sync-up by sending the DMD a forced sync signal. This will not place the nodes into mode '3' any faster, but will allow you to attempt provisioning some nodes, while other nodes are in the process of syncing up.

Step 1 Execute command **selnd** from the CWM command line. Note the nodes in mode 3. Connections provisioned after forced sync-up can only go through nodes with mode = 3.

Step 2 Send the sync-up signal to the DMD by entering command **kill -ALRM dmd**.

Step 3 View the .DBKR_SYNCUP_MESSAGE file for the sync-up completion.

J.10.8.4.6 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "No more vpi/vci available for local trunk end" Error

Related key index entries: cmgrd, sdbroker, vpi/vci

Provisioning fails and the following error messages are displayed:

- "No more vpi/vci available for local trunk end" and "Remote trunk"
- "Local end of the connection already exists," "Remote end," and "Both end"
- "Vpcon already exists for Local Vpi," "Remote Vpi," and "Both ends"

Each of these error messages identifies the reason for the failure of provisioning. They sometimes can be displayed in error. The reason is a mismatch between the switch and the DMD's cache. To find out if a mismatch has occurred, dump the DMD cache, using the command **pkill -USR1 dmd** and compare the values in the cache with those on the switch for endpoints associated with the error.

Defect Information—If the switch and DMD cache are not in sync, you will need the DMD logs, message logs, DMD cache dump, and the EM logs for the node in question. You will also need the switch CLI screen shot of the connection in question.

Possible alternative workaround—If there is a cache inconsistency, the only workaround is a complete cache resync (/opt/svplus/tools/CacheResync). If there is no DMD cache inconsistency, it is a normal operational scenario. Different connection add parameters should be chosen.

J.10.8.4.7 Cmgrd—Sdbroker Addition Errors: Adding a Connection Results in "EndPoint Exists Local/Remote/Both end of the connection already exists." Error

Related key index entries: cmgrd, sdbroker, endpoint exists

During an add connection request, the cmgrd will request intermediate endpoint vpi/vci from sdbroker. If the sdbroker incorrectly chooses endpoints that are already in use by the switch the cmgrd will try to provision these endpoints and return the error "endpoint exists" to the user.

Step 1 Determine which of the endpoints already exist on the switch. (If it is the intermediate endpoints then it is an sdbroker problem.)

a. When provisioning hybrid connections the CMGRD requests intermediate endpoints from the sdbroker. The sdbroker then requests them from DMD and then sends them back to CMGRD. First use the **dbcmap** command (/opt/svplus/tools/dbcmap) to identify the DMD that is used to process the node. Then dump that DMD's cache. Verify that the DMD does not contain the endpoints in question in its cache.

b. Determine why the DMD doesn't have the information on endpoints that exist on a switch. You first need to determine if the EM sent the add message to the DMD. See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129. If the add message is not found and the logs do not go back to coldstart, then you will need to check to see if the EM has done any processing of this endpoint. Check for the endpoint in the xxx_Connection table. If the endpoint is not there, check the EM to determine why it did not process the endpoint. If the endpoint is in the xxx_connection table, you know that the EM processed it, but you do not know if it forwarded it to the DMD.

Defect Information:

- If the problem is an intermediate endpoint and it is on the switch, but the EM didn't process it or didn't' send the message to DMD, check the EM log and nts log from /opt/svplus/log.
- If the problem is within the DMD you will need the DMD logs, DMD message logs, and the DMD cache dump.

Possible alternative workaround—None.

J.10.8.4.8 Cmgrd—Sdbroker Modification/Deletion Errors: Modifying or Deleting a Connection Results in "sDatabroker Could not lock connection entry." Error

Related key index entries: cmgrd, sdbroker, lock connection

During a modify or delete connection request, this error could result if sdbroker cannot find the connection in its cache.

All scenarios of modify/delete connection failures display the same error. To determine exactly what happened you must view the /opt/svplus/log/sdbrokerX.XXXX.log file.

Step 1 Search for the error "<sDbkr_CmgrdModConn_c::Process> INTERFACE ERROR" near the end of the file. A detailed reason for the error will follow on the same line.

Note For delete connection requests, search for sDbkr_CmgrdDelConn_c::Process instead of sDbkr_CmgrdModConn_c::Process.

Defect Information:

- If the problem is an intermediate endpoint and it is on the switch, but the EM didn't process it or didn't send the message to DMD, check the EM logs and nts logs from /opt/svplus/log.
- If the problem is within the DMD, you will need the DMD logs, DMD message logs, and the DMD cache dump.

Possible alternative workaround—None.

J.10.8.4.9 Cmgrd Errors

During an addition request, cmgrd could return errors which cmgrd has received from snmpcomm or the switch itself.

J.10.8.4.10 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Fail due to Switch Timeout" Error

Related key index entries: cmgrd, timeout

When any add, modify, or delete connection request is made, cmgrd issues a request to the switch with an SNMP community string, either a SET or GET string. These community strings are overwritten by the process snmpcomm. This process uses the values of the strings which are present in the node_info table. Thus, when a provisioning request times out from the switch, one possible problem is that the node's community string in the node_info table does not match the string on the node itself.

The problem can be researched by checking the community strings on the node and the node_info table.

Step 1 Check the community strings on the nodes by issuing the command **dsnmp**.

Step 2 Check the community string in the node_info table based on node_id. The strings are encrypted, so use the decrypt binary, which displays the string in the Clear format.

Step 3 Once the strings are cross-referenced and you have determined that a discrepancy is indeed present., then you can change the strings in either of the following ways:

- Issue the command **cnfsnmp** on the node and change the community strings to match that of the CTM.

- Use the RunConfigurator process to change the string in the CTM to match that of the switch.

Defect Information—If these methods do not work, collect the following:

- Cmgrd.log located in the /opt/svplus/cmgrd.log directory
- The output of the query "select (*) from node_info where node_id = X"

J.10.8.4.11 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Agent not responding, request timed-out; or Fatal error, Snmpcomm is not running." Error

Related key index entries: cmgrd, snmpcomm

When any add, modify, or delete connection request is made, cmgrd issues a request to the switch, but the request is actually first issued to the process snmpcomm, which in turn sends the SNMP SET/GET to the node. In this scenario, these errors can be returned by the process snmpcomm or the error could be a time out error from the snmpcomm process or an ILOG communication error.

The reason that snmpcomm can send a timeout error is because it is too busy processing requests and cannot accept more requests at the moment. The reason for the "SnmpComm not Running" error is that cmgrd could not establish an ILOG connection with it.

Step 1 Issue the command **psg snmpcomm** to ensure that the process is indeed running.

Step 2 Check for snmpcomm coredumps in the corefilesdir directory.

Reissuing the request after waiting for few minutes will take care of the timeout error.

If you confirm that the snmpcomm process is not running, then you must do a warmstart to ensure that the process comes up. When the process starts the ILOG connection with cmgrd is established.

Defect Information:

- If you get the same timeout error after reissuing the request, then collect the cmgrd.log and snmpcomm.log.
- If the snmpcomm process does not run after a warmstart, then collect the watchdog.log file.

Possible alternative workaround—Reissue the request after waiting a while. This interval could enable snmpcomm to clear its pending requests. Do a warmstart to ensure that the snmpcomm process starts up.

J.10.8.4.12 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Outstanding request exists for same object." Error

Related key index entries: cmgrd, outstanding request

When any add, modify, or delete connection request is made, cmgrd processes these requests in a multithreaded manner. Sometimes a request can take longer than 3 minutes to process, because of the different scenarios that the switch responds with (for example, timeouts). If the request takes longer than 3 minutes from the CM GUI, then the GUI will timeout and indicate this to the user. From the Connection Proxy path the timeout value is 2 minutes, after which it will indicate a timeout error.

If you reissue this request immediately, cmgrd could return the error "Outstanding requests exists for the same object."

The reason this error is returned is because cmgrd is still processing the initial request which the clients (CM GUI and Connection Proxy) timed out on. An ideal case for this would be when a switch timeout is received for a multisegment case, and cmgrd is still busy backing off other segments and waiting for the timeout response of additional segments. Just to be sure that cmgrd is still running, issue the following commands.

Step 1 Issue the command **psg cmgrd** to ensure that the process is indeed running.

Step 2 Check for cmgrd coredumps in the corefilesdir directory. If there indeed was a coredump collect the corefile.

Step 3 Execute **tail -f cmgrd.log** in the logs directory to see if cmgrd is processing requests.

Reissue the request after waiting for a few minutes.

Defect Information—If you get the same timeout error after reissuing the request, then collect the cmgrd.log.

Possible alternative workaround—Reissue the request after some time, this interval could enable cmgrd to clear its pending request.

J.10.8.4.13 Cmgrd—Addition/Modification/Deletion Errors: Provisioning a Connection Results in "Fatal error, IOSMGR is not running, may need to be manually started" Error

Related key index entries: cmgrd, iosmgr

When any add, modify, or delete connection request is made with a Popeye1 RPM Card, cmgrd issues a request to the switch, but the request is actually first issued to the process iosmgr, which in turn sends the request to the node, via an expect script session. In this scenario, this error can be returned when cmgrd cannot talk to iosmgr via the ILOG connection.

The reason for the error is that cmgrd could not establish an ILOG connection with iosmgr.

Step 1 Issue the command **psg iosmgr** to ensure that the process is indeed running.

Step 2 Check for iosmgr coredumps in the corefilesdir directory.

If you determine that the iosmgr process is not running, then you must do a warmstart to ensure that the process comes up. When the process starts, the ILOG connection with cmgrd is established.

Defect Information—If the iosmgr process does not run after a warmstart, then collect the runiosmgr.log file.

Possible alternative workaround—None. Iosmgr has to be running to be able to provision on Pop1 RPM cards.

J.10.8.4.14 Cmgrd—Addition Errors: Provisioning a Connection Results in "Vpi/vci ranges retrieval from svc_operation failed" Error

Related key index entries: cmgrd, svc_operation

This error is only present for a hybrid connection add request. cmgrd queries the svc_operation table of the feeder trunk ports for the vpi/vci ranges. These ranges in turn are given to the sdbroker, which in turn returns an available vpi/vci that cmgrd uses to set on this feeder trunk port.

The reason for the error is that when cmgrd queries the svc_operation table for the feeder trunk port's vpi and vci ranges, the entry is not found in the table.

Step 1 Reissue the hybrid connection add request but tail the cmgrd.log.

Step 2 In this log a query in the form of "SELECT MIN_SVCC_VPI, MAX_SVCC_VPI, MIN_SVCC_VCI, MAX_SVCC_VCI FROM SVC_OPERATION WHE RE NODE_ID = X AND SLOT = X AND PORT + 1 = X" will be seen. This is the actual query that is failing.

Step 3 Run the query from the command line or dbaccess stratacom prompt to figure out which port's information is not present in the svc_operation table. The reason could be that for that port the resource partition is not configured on the CLI. Go to the CLI and issue the command **addpart** for that port.

Step 4 After issuing the command **addpart** on the CLI, check the CTM table svc_operation database for the existence of the row. If the row is present the connection request can be reissued. If the row still is not present in the svc_operation then it is a probably an EM issue.

Defect Information—If after configuring the resource partition on the CLI, and the svc_operation table is still not populated then see J.10.4 Equipment Management Problems, page J-40 and collect the appropriate ooemc logs.

Possible alternative workaround—None.

J.10.8.4.15 Cmgrd—Addition/Modification/Deletion Errors: Provisioning a Connection Results in "Can't get segment info from Data-base." Error

Related key index entries: cmgrd, segment info

This error is returned by cmgrd when it cannot get a row from one of the CTM database tables for the current connection request. If the request is an add, then the query for the intermediate endpoints from either the node or the bis_object tables may have failed. If it is a Mod/Del then in addition to the failure of the queries into the node and bis_object tables, the problem could be that the connection is not found in the user_connection table.

In this error scenario there could be multiple reasons of failure that differ between add and modify/delete requests. But most of the time this error is returned if one of the queries to the node, bis_object, and user_connection tables fails for the current request. Some basic checks would be to see if the nodes in question and in the intermediate nodes are really synced up with CTM. You should also try the same request from both the CM GUI and Connection Proxy paths.

Because of the nature of this error it is best that a CTM DE investigate.

Defect Information—Collect cmgrd.log, cmsvr.log, ConnProxy*.log, and sdbroker*.log.

Possible alternative workaround—None.

J.10.8.4.16 Cmgrd—Switch Errors

During an addition, modification, or deletion request, cmgrd sends SNMP requests to the switch. When the switch rejects an SNMP request, cmgrd queries the Error MIB table and gets the error string to display.

J.10.8.4.17 Cmgrd—Addition and Modification Errors: Provisioning a Connection Results in "Agent reported bad/wrong value for one of the variables in the request." Switch Error

Related key index entries: cmgrd, bad value

When any add or modify connection request is issued, an SNMP VarBind is set on the switch via cmgrd. The switch can reject this VarBind with this error.

The reason for the error is that cmgrd sent an invalid value for one of the MIB objects. The CTM DE should do the investigation for this error, as it indicates that there is a problem in the data that cmgrd either received from the clients or internally mapped from the other side of the connection.

Try the same connection from both the Connection Proxy and CM GUI interfaces and note the behavior from both of the clients. If the provisioning result from both clients is the same, it tends to indicate that this is either a cmgrd issue or a sdbroker vpi/vci issue.

Defect Information—The cmgrd.log, ConnProxy*, cmsvr.log and sdbroker*.logs should be collected.

Possible alternative workaround—If you are doing an add and you are using default values, then there is no workaround. However, if you are doing a modify, you can change the value of the object being modified and retry the connection. Also, if this is a sdbroker vpi/vci issue, retry the connection, because sdbroker does not reuse the previous vpi/vci combination.

J.10.8.4.18 Cmgrd—Addition Errors: Provisioning a Connection Results in "Object Exists on the Agent or Specified VPI/VCI not available." Switch Error

Related key index entries: cmgrd, object exists

When any add connection request is issued, an SNMP VarBind is set on the switch via cmgrd. The switch can reject this VarBind and the subsequent cmgrd query to the switch error table can return these errors.

The reason for the error is that the connection that CTM is trying to add already exists on the switch. This could be a user endpoint or an intermediate endpoint.

Step 1 Retry the same connection. If this second attempt succeeds it indicates that the intermediate endpoint's vpi/vci was already present on the switch. If this is the case, look at the cmgrd-sdbroker error "EndPoint Exists Local/Remote/Both end of the connection already exists."

Step 2 If the switch returns the same error on the second attempt, this could indicate an inconsistency between the CTM database and the switch, and it must be debugged by a CTM DE.

Defect information—Save the cmgrd.log, ConnProxy*.log, cmsvr.log and sdbroker*.log.

Possible alternative workaround—Retry the connection addition more than once. If it still fails, a CTM DE will have to look into the issue.

J.10.8.4.19 Cmgrd—Addition/Modification Errors: Provisioning a Connection Results in "Requested cell rate (lscr/lpcr or rpcr/rscr) is too high" Switch Error

Related key index entries: cmgrd, cell rate

During an add or modify connection request, it is possible that the port the connection is being set on has no more resources available to accept the traffic parameters that the current SNMP SET is requesting. At this point, the switch will reject the request and return this error.

Step 1 For the user endpoint, check the user port on the CLI using the command **dsppnportrsrc**. This will indicate the resources available per port.

Step 2 If the failure is not happening on a user endpoint port, but instead on an intermediate port (for example, for multisegment connections), find out the local and remote endpoint feeder trunk ports. (This can be done by using the Network Topology GUI.)

Step 3 On the CLI, execute the **dsppnportrsrc** command to check for the feeder trunk ports.

Defect information—If you continue to receive this error after you have verified that the ports have enough bandwidth to add these connections, save the cmgrd.log.

Possible alternative workaround—Freeing up resources on the port which needs the bandwidth to add the connection, or lowering the traffic parameters value in the connection request.

J.10.8.4.20 Cmgrd—Addition Errors: Provisioning a Connection Results in "SPVC is not allowed on this interface" Switch Error

Related key index entries: cmgrd, interface

During an add connection request, it is possible that the user endpoint port that the connection is being set on, has an incorrect signaling configured on it. This error is indicative of this condition.

For nontrunking ports the signaling on the port cannot be PNNI.

Step 1 For the user endpoint, do the following:

a. Use the **dsppnport** command to verify that the interface is a PNNI port or a controller port.

b. Change the port to a UNI port. Before doing this make sure that no calls are going through this interface.

```
dnpnport <portID>
cnfpnportsig <portID> -univer uni30
```

Step 2 After changing the configuration retry the connection request.

Defect Information—Not applicable, as this error has to be a switch configuration issue.

J.10.8.4.21 Cmgrd—Addition Errors: Provisioning a Connection Results in "Local Channels not enough." Switch Error

Related key index entries: cmgrd, channels

During an add connection request, it is possible that the user endpoint port or card that the connection is being set on, has already reached its limit of allowable connections.

Check the port or card of the user endpoints on the CLI.

Step 1 Check the port resources of the endpoint using the **dsppnportrsrc**.

Step 2 If the number of LCNs is zero, delete some connections from this interface.

Step 3 After changing the configuration retry the connection request.

Defect Information—Not applicable, as this error has to be a switch configuration issue.

J.10.8.4.22 Cmgrd—Addition and Modification Errors: Provisioning a Connection Results in "Error in Traffic Parameters." Switch Error

Related key index entries: cmgrd, traffic parameters

During an add or modify connection request, if the local endpoint's remote parameters do not match the remote endpoint's local parameters, then this error is indicated by the switch. The particular parameter depends on the service type of the connection.

Note This error cannot be easily debugged. I just has to be checked by a Connection Management DE, because the error indicates that the mapping of local to remote (and/or remote to local) has a problem in the value that is being set on the switch.

Step 1 Retry the connection from both the CM GUI and Connection Proxy interfaces.

Step 2 If the result from both the interfaces is the same, this could be a cmgrd bug. If the request succeeds from one of the interfaces, then this is more likely a client issue.

Defect Information—Collect cmgrd.log, ConnProxy*.log, and cmsvr.log.

Possible alternative workaround—Change some of the traffic parameter values in the connection request and retry the connection.

J.10.8.4.23 Cmgrd—Addition, Modification, and Deletion Errors: Provisioning a Connection Results in "Network Busy, try later" Switch Error

Related key index entries: cmgrd, network busy

During an add or modify connection request, if the switch returns this error, it indicates that there is some CPU-intensive activity happening on the controller card. The cmgrd request will be backed off the other segments and this error will be returned. However, the operation is not backed off for a delete operation, because this is a destructive command.

There is no workaround for this error. You will have to wait and retry the request later. If you continue to receive the error after waiting and retrying multiple times, then the problem must be checked from the switch side.

Defect Information—Not applicable.

Possible alternative workaround—Wait and try the connection at a later time.

J.10.8.4.24 Cmgrd—Modification Errors: Modifying a Connection Results in "Connection does not exist in CproDb/Agent returned no such name" Switch Error

Related key index entries: cmgrd, cprodb

During a modify connection request, the switch could return this error when the connection is truly not present on the switch.

Check the connection in the user_connection table. From this entry, verify that all of the segments do exist on the switch CLI. If all segments are truly present in the switch CLI then the issue must be checked from the switch side. However, if any of the segments is not present on the switch, then this could be a sdbroker or EM issue.

Defect Information—If it is deemed a sdbroker or EM issue, collect the appropriate logs and cmgrd.log. If all of the segments of the connection are present on the switch and the switch still returns this error, contact the switch DEs.

Possible alternative workaround—None.

J.10.9 Diagnostics Center Problems

The Diagnostics Center provides different diagnostics operations at the following different network elements levels.

- Network Diagnostics
  - Retrieve the current sync status and alarm status of all the nodes in the network.
  - Support the network/node health statistics and manageability checks. At the network level, only the node manageability check results are supported.
- Node Diagnostics
  - Retrieve current sync status, node alarm status, IP address, and several other node attributes.
  - Retrieve the sync status of all the cards in the node.
  - Request a node resync.
  - Request VSI partition data and also perform VSI consistency checks on the node.
  - Support node health statistics such as SNMP success counts and FTP/TFTP success/failure counts.
  - Perform node manageability checks such as IP reachability and SNMP community string checks.
- Card Diagnostics
  - Retrieve card-level information (such as sync status, card status, and firmware revision)
  - Retrieve card CPU usage on cards that support this functionality
  - Retrieve the memory pool usage information on cards that support this functionality
  - Retrieve the memory buffer pool usage Information on cards that support this functionality
  - Retrieve card-level, real-time statistics, if any
  - Retrieve information about all lines and paths that are in loopback on the card
  - Retrieve information about currently running BERT tests on the card
  - Retrieve information about currently running IMA link tests
- Port Diagnostics
  - Retrieve the port-level attributes such as port status
  - Perform loopback
  - Perform start/stop/modify BERT
  - Retrieve the results and/or current status of the BERT
  - Monitor the scheduled grooming results
  - Configure the on-demand grooming
  - Retrieve the port-level, real-time statistics
- Line Diagnostics
  - Retrieve the line-level attributes such as line status and loopback status
  - Perform loopback
  - Perform start/stop/modify BERT
  - Retrieve the results and/or current status of the BERT

  - Retrieve the line-level, real-time statistics
- Path Diagnostics
  - Retrieve the path-level attributes such as path status
  - Perform loopback
  - Retrieve the path-level, real-time statistics
- Trunk Diagnostics
  - Retrieve the trunk-local and remote-end, real-time statistics
- IMA Group Diagnostics
  - Retrieve the IMA group-level attributes such as IMA group status
  - Retrieve the accumulated delay on all the IMA links under the IMA group
  - Clear the accumulated delay on all the IMA links under the IMA group
  - Restart the IMA group
  - Retrieve the IMA group ATM cell layer ingress/egress counters
  - Retrieve the IMA group-level, real-time statistics
- IMA Link Diagnostics
  - Retrieve the IMA link-level attributes such as IMA link status
  - Start/stop IMA link test
  - Modify IMA link test pattern
  - Retrieve the IMA link-level, real-time statistics
- Connection Diagnostics
  - Retrieve the connection-level attributes such as connection status
  - Retrieve the local and remote endpoint attributes such as A-bit, AIS, and OAM
  - Retrieve the local and remote endpoint real-time statistics

The Diagnostics Server interfaces with the CM Server to support the following connection-related diagnostics operations:

- Connection loopback
- Up connection
- Down connection
- Connection trace
- Test connection
- Test delay
- Test connection segment
- Test ping OAM

J.10.9.1 Diagnostics Center Framework

This section includes the following information:

- J.10.9.1.1 Cannot Launch Diagnostics Center, page J-109
- J.10.9.1.2 Cannot Launch Other Applications from the Diagnostics Center, page J-109

- J.10.9.1.3 An Exception Is Raised when the Diagnostics Center Is Launched, page J-110
- J.10.9.1.4 Double-Click Operation In Diagnostics Center Tree View Does Not Launch an Internal Frame, page J-110
- J.10.9.1.5 Drag-and-Drop Functionality Errors Within the Diagnostics Center, page J-110
- J.10.9.1.6 Drag and Drop from/to Diagnostics Center to/from Other Applications, page J-111
- J.10.9.1.7 Drop Target Displays Incorrect Object or Object Data, page J-111
- J.10.9.1.8 Diagnostics Center Does Not Respond (GUI Is Grayed Out), page J-111

J.10.9.1.1 Cannot Launch Diagnostics Center

The Diagnostics Center cannot be launched (main window will not appear) using one of the following methods:

- Click the **Diagnostics Center** icon from the Launch Center or from any application.
- Choose **Tools > Diagnostics Center** from any application.
- Right-click the selected node from the hierarchical tree, and choose **Diagnostics Center**.

Step 1 Check diagcenter.jar file under /opt/svplus/java/jars/cwm directory.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCSserver.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.2 Cannot Launch Other Applications from the Diagnostics Center

The Diagnostics Center cannot launch other applications using one of the following methods:

- Choose the target application under the **Tools** menu item.
- Right-click on the selected object from the hierarchical tree, and choose the target application.

Step 1 Check the target application jar file. Make sure the target application jar file exists under the /opt/svplus/java/jars/cwm directory on the target machine.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.3 An Exception Is Raised when the Diagnostics Center Is Launched

When the Diagnostics Center is launched using one of the following methods, an exception is raised and the Java Console shows the exception trace information.

- Choose the target application under the **Tools** menu item.
- Right-click on the selected object from the hierarchical tree, and choose the target application.

Defect Information—Collect the following information for further analysis:

- Java Console information.
- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.4 Double-Click Operation In Diagnostics Center Tree View Does Not Launch an Internal Frame

Double-clicking on an object in the Diagnostics Center tree view does not launch an internal frame in the content window to open the object in the context pane (internal frame).

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Java Console information.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.5 Drag-and-Drop Functionality Errors Within the Diagnostics Center

The drag-and-drop functionality of a network element from the Diagnostics Center tree view to the content pane (a) fails to open an internal frame or recycle the contents of an existing frame to display the object's attributes or (b) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine if the drag-and-drop functionality is supported for the dropped object.

The following objects can be dropped from the tree view to the Diagnostics Center content pane:

- For the Element tab, the Network, Node, Card, Line, Port, IMA, and IMA links objects are supported and 'Folder' objects are not supported.
- For the Connection tab, the Node, Card, Line, Port objects are supported and Folder, IMA, and IMA link objects are not supported.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.

- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.6 Drag and Drop from/to Diagnostics Center to/from Other Applications

As a drag source, the drag-and-drop functionality of an object from the Diagnostics Center to another CTM application fails to display the selected object in the target application.

As a drop target, the drag-and-drop functionality from another application to the Diagnostics Center's content pane (a) fails to open an internal frame or recycle the contents of an existing frame to display the dropped object's attributes or (b) results in the 'Operation Not Supported' message dialog box.

Step 1 Determine whether the drag-and-drop functionality is supported for the selected object.

Step 2 Determine whether the target application supports the drag-and-drop functionality for the dropped object.

Step 3 Determine whether the source and the target application belong to the same instance of the Java VM. CTM framework does not support drag-and-drop functionality across applications belonging to different Java VMs.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.7 Drop Target Displays Incorrect Object or Object Data

The Diagnostics Center's internal frame opens successfully, but either it displays either information related to another object or the dropped object attribute values are not correct.

Defect Information—Collect the following information for further analysis:

- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.1.8 Diagnostics Center Does Not Respond (GUI Is Grayed Out)

Step 1 Determine whether a Java DOS window has already been enabled.

a. Launch the WebStart application.

b. Click on **File > Preferences**.

c. Select the **Java** tab.

d. For the selected Java entry, check the Command column entry (If needed, expand the column to display all information) to determine if it is set to javaw.exe or java.exe.

e. If the Command column setting is set to java.exe, then the Java DOS window is already enabled and a DOS window task should be running on the machine. Otherwise, the Java DOS window is not enabled (Command column entry is set to javaw.exe).

Step 2 If the Java DOS window is already enabled, collect defect information.

Step 3 If the Java DOS window is not enabled, then the current log information might not be sufficient to determine the root cause.

a. Collect currently available log information.

b. Enable the Java DOS window by changing the'javaw.exe' to'java.exe'.

c. Verify that the WebStart/Java DOS is enabled.

d. Use the PC client to launch a GUI application and verify that a DOS box has been launched.

e. Try to reproduce the problem in order to collect additional Java-related data using the WebStart/Java DOS window.

Defect Information—Collect the following information for further analysis:

- Java DOS window data:
  - Select the Java DOS box.
  - Issue a Ctrl and Break command. Hold the **Ctrl** key down and click on the **Break (Pause)** key. This action should result in the DOS window showing Java thread-related information.
  - Copy the data to a log file for further analysis.
- CMSCclient.log file under the D:\Documents and Settings\<username>\log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- Cmsvr.log file under the /opt/svplus/log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.2 Diagnostics Center Server-Specific Issues

This section includes the following information:

- J.10.9.2.1 XML Parser Error, page J-113
- J.10.9.2.2 SNMPCOMM_TIMEOUT Error While Polling MIB Objects, page J-113
- J.10.9.2.3 Node Sync-Up Status Are Not Shown in the Diagnostics Center, page J-114
- J.10.9.2.4 Node Resync Fails, page J-114
- J.10.9.2.5 Polling of Real-Time Counters Fails, page J-114
- J.10.9.2.6 Some Real-Time Counters Are Not Shown, page J-115
- J.10.9.2.7 Unable to Start, Stop, or Modify BERT Operations, page J-115
- J.10.9.2.8 Unable to Start/Stop IMA Link Test Patterns, page J-116
- J.10.9.2.9 Cannot Perform Connection Diagnostics, page J-116
- J.10.9.2.10 Miscellaneous Issues or Problems in Diagnostics Center, page J-117

J.10.9.2.1 XML Parser Error

The XML parsing error is seen while launching the Diagnostics Center (either by the drag-and-drop method or the right-click method) for a network element. The popup window says "Internal Error: XML Parsing Error."

Step 1 Verify whether the entity (node, card, line, or port) that caused this error is supported in the CTM version being used. If this error is seen for a supported node/card, go to step 2.

Step 2 Open the /opt/svplus/log/DCServer.log file and look for the message information from when this error occurred.

a. A typical message in the log looks like this:

```
ERR: Fatal Error at file, line 0, char 0, Message: An exception occurred!
Type:RuntimeException, Message:The primary document entity could not be opened.
Id=/opt/svplus/xml/diagcenter/XXX/XXX-XXX.xml ( <someNumber>: <x>) <someTime Stamp>
ERR: InternalError: XML Parsing Error
```

b. If the .xml filename mentioned previously has two consecutive hyphens (for example: ABC--XYZ.xml), or if it has a preceding hyphen (for example: -ABC.xml) or terminates with a hyphen before the file extension (for example: ABC-.xml), proceed to step 3, where investigating incorrectly formatted XML filenames is discussed.

c. See if the .xml file mentioned in the log message (as shown in the previous substep) exists under the /opt/svplus/xml/diagcenter directory. If it does not exist, contact the CTM engineers with the defect information.

Step 3 Perform the following substeps to investigate incorrectly formed XML filename strings. The format of XML filenames is <Platform>-<Card>-<InterfaceType>-<SomeEntityName>.xml. This format is generic with a few exceptions. Also note that Platform and InterfaceType are optional and will not be seen in many files (for example: ABC-Card.xml is a valid XML filename).

a. If the Platform part of the XML filename is incorrect/missing, check the Node table to see if it is correctly populated.

b. If the Card part of the XML filename is incorrect/missing, check the Card table to verify if it is correctly populated.

c. If the InterfaceType part of the XML filename is incorrect/missing, check the appropriate table to verify if it is correctly populated. This table generally corresponds with the line/port table of the card for which this error is noticed.

d. If the EntityName part of the XML filename is incorrect, contact the CTM engineers with the defect information required.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots for the investigative commands used for debugging this issue.
- DCServer.log file from the log directory.

Possible alternative workaround—None.

J.10.9.2.2 SNMPCOMM_TIMEOUT Error While Polling MIB Objects

The Diagnostics Center shows an SNMP timeout error when polling real-time counters.

Step 1 Check the status of the node.

Step 2 If the node is reachable then check whether the community strings are set properly.

Step 3 Check the DCServer.log file to determine whether the community string used for querying the objects is set correctly.

Step 4 Check whether the query has been sent to the switch.

Defect Information—Collect the following information for further analysis:

- CMSClient.log file under the D:\Documents and Settings\<username>\log directory.
- DCServer.log file under the /opt/svplus/log directory.

Possible alternative workaround—None.

J.10.9.2.3 Node Sync-Up Status Are Not Shown in the Diagnostics Center

When the Diagnostics Center is launched for a network element, it does not show the node sync-up status for all the nodes in the network.

Step 1 Run selnd as svplus and check the status of all the nodes. If they are not shown properly, then there is probably a problem with the EM process. Check the EM logs.

Step 2 Check the node table entries for all the nodes.

Defect Information—Collect the following information for further analysis:

- Node table entry for the corresponding node.
- DCServer.log file from the log directory.

Possible alternative workaround—None.

J.10.9.2.4 Node Resync Fails

Node resync fails from the Diagnostics Center.

Step 1 Check whether the node is reachable.

Step 2 Check for any exceptions in the DCServer.log file.

Defect Information—Collect the following information for further analysis:

- Node table entry for the corresponding node.
- DCServer.log file from the log directory.
- Emd.log from the log directory.

Possible alternative workaround—None.

J.10.9.2.5 Polling of Real-Time Counters Fails

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether the real-time counters are applicable. Check any appropriate commands from the CLI.

Step 3 Use any SNMP tool and check whether the MIB objects are retrievable.

Step 4 Narrow down the problem by selecting one counter at a time and determining for which counters the polling fails.

Defect Information—Collect the following information for further analysis:

- DCServer.log file from /opt/svplus/log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- CLI output of dspcd <slot No> for that card. Output of any appropriate CLI commands used.
- If step 4 was performed, provide the list of counters for which polling failed.

Possible alternative workaround—Use the CLI to monitor the real-time counters.

J.10.9.2.6 Some Real-Time Counters Are Not Shown

Some real-time counters are missing from the Diagnostics Center.

Step 1 Check whether the counters are applicable to the card (version/mode if applicable).

Step 2 Check any appropriate commands from the CLI.

Step 3 Use any SNMP tool and check whether the MIB objects are retrievable.

Defect Information—Collect the following information for further analysis:

- DCServer.log file from /opt/svplus/log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.
- CLI output of dspcd <slot No> of the card.
- List of missing counters for the particular node/card.

Possible alternative workaround—Use the CLI to get the real-time counter values.

J.10.9.2.7 Unable to Start, Stop, or Modify BERT Operations

Unable to start, stop, or modify BERT operations from the Diagnostics Center.

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether the card is in the Active state.

Step 3 Check whether the correct VarBinds have been sent for snmpset.

Step 4 Check whether the options set for start/stop/modify BERT are applicable.

Step 5 Check whether the BERT operations are successful in the CLI with the options chosen from the Diagnostics Center.

Step 6 The Diagnostics Center sends only the mandatory and modified values to the Diagnostics Center server for snmpset. Use any SNMP tool with these values alone and perform a BERT operation. If it succeeds, then there is some problem with the Diagnostics Center.

Defect Information—Collect the following information for further analysis:

- DCServer.log file from /opt/svplus/log directory.
- Screen snapshots; in particular, the Diagnostics Center BERT window, error/information messages dialog boxes.

Possible alternative workaround—Use the CLI/DiagProxy for BERT operations.

J.10.9.2.8 Unable to Start/Stop IMA Link Test Patterns

Unable to start/stop/modify IMA Link Test pattern from the Diagnostics Center.

Step 1 Check whether the node is reachable and the community strings are set correctly.

Step 2 Check whether the card is in the Active state.

Step 3 Check whether the correct VarBinds have been sent for snmpset.

Step 4 Check whether the IMA Link Test pattern can be performed from the CLI.

Step 5 Use any SNMP tool and try to set the objects shown in the DCServer.log file.

Defect Information—Collect the following information for further analysis:

- DCServer.log file from /opt/svplus/log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.

Possible alternative workaround—Use the CLI for IMA Link test patterns operations.

J.10.9.2.9 Cannot Perform Connection Diagnostics

The connection diagnostics are performed through the CM Server application. The Diagnostic Server forwards all the connection diagnostics requests to the CM Server. If there are any connection diagnostics errors, they are more likely to be in the CM Server application.

Step 1 Check whether the sync up is complete.

Step 2 Check whether the node is reachable and the community strings are set correctly.

Step 3 Check whether the card is in the Active state.

Step 4 Check whether the correct VarBinds have been sent for snmpset.

Step 5 Check for any specific exceptions in the DCServer.log file.

Step 6 If there are no exceptions in the DCServer.log file, then the problem could be originating in the Connection Manager.

Defect Information—Collect the following information for further analysis:

- DCServer.log and cmsvr.log files from /opt/svplus/log directory.
- Screen snapshots; in particular, error/information messages dialog boxes.

Possible alternative workaround—Use the CLI or SNMP conn proxy for connection diagnostics.

J.10.9.2.10 Miscellaneous Issues or Problems in Diagnostics Center

If you encounter any other issues or problems, contact the CTM engineers with the defect information.

Step 1 Check whether a similar operation can be performed successfully through the CLI.

Defect Information—Collect the following information for further analysis:

- Describe the operation during which the problem/issue was encountered.
- DCServer.log and cmsvr.log files from /opt/svplus/log directory.
- Screen snapshots.
- CLI dump of this operation if applicable.

Possible alternative workaround—None.

J.10.10 Performance Management Collection and Parsing Problems

PM collection is done on the entire node and statistics files are uploaded from all applicable cards on that node.

The Stats Parser parses these statistics files and stores the stats data in the database.

J.10.10.1 PM Collection Issues

This section includes the following information:

- J.10.10.1.1 pmcollector—Generic Troubleshooting, page J-117
- J.10.10.1.2 PM Collection Fails for the Node—Log File Shows "Node not discovered", page J-118
- J.10.10.1.3 PM Collection Fails for the Node—Log File Shows "Card not discovered", page J-118
- J.10.10.1.4 PM Collection Fails for the Node—Log File Shows "Time not synchronized", page J-119
- J.10.10.1.5 PM Collection Fails for the Node—Log File Shows "Snmp failed", page J-119
- J.10.10.1.6 PM Collection Fails for the Node—Log File Shows "Ftp failed", page J-120
- J.10.10.1.7 PM Collection Fails for the Node—Log File Shows "Polling failed and wait for major retry" or "Major retry failed and wait for critical retry" or "Critical retry failed and wait for history retry" or "History retry failed and wait for next retry" or "No more retry", page J-120

J.10.10.1.1 pmcollector—Generic Troubleshooting

When performing generic troubleshooting, always do the following:

- Verify that the pmcollector process is running by executing the **psg pmcollector** command and checking for a result.
- Make sure the stats files are in the /opt/svplus/purge directory of CTM. Check for all stats files; there should not be any missing file, and there should be no files accumulated in the /opt/svplus/spool directory.
- Check the file_err_log table for any file collection failure.

- Check the collsvr_err_log table for any failure during start/stop collection.
- Check the coll_err_log table for entire collection server errors.
- Check '/opt/svplus/cache/scm/scmcollout.log' for a completed stats file request.
- Check '/opt/svplus/cache/scm/scmcollin.log' to verify whether or not stats file has been completed.
- Check '/opt/svplus/cache/scm/scmcollout.log' for stats file collection errors.

J.10.10.1.2 PM Collection Fails for the Node—Log File Shows "Node not discovered"

This can happen when the node is not in mode 3.

Step 1 Check the node_info table by executing the following command:

```
echo "select node_not_discovered from node_info where node_id=<node_id> and slot=<slot>" |
dbaccess
```

If node_not_discovered is set to 1, it means that the node has not been discovered.

Step 2 Check the state of the node by executing the following command:

```
echo "select (*) from node where node_name=<node-name>" | dbaccess
```

Step 3 Check the mode of the node in the output: the mode must be 3.

Defect Information—Collect the following information for further analysis:

- pmcollector.log, output of selnd or output of:

  ```
  echo "select (*) from node where node_name = '<node-name>' " | dbaccess
  ```

- Related key index entries
- pmcollector

Possible alternative workaround—If the node is not mode 3, look up troubleshooting for the EM module.

J.10.10.1.3 PM Collection Fails for the Node—Log File Shows "Card not discovered"

This can happen when the card is not in the Active state.

Step 1 Check the node_info table by executing the following command:

```
echo "select card_not_discovered from node_info where node_id=<node_id> and slot=<slot>" |
dbaccess
```

If card_not_discovered is set to 1, it means that the card has not been discovered.

Step 2 Check the card table by executing the following command:

```
echo "select fc_state, fc_type, slot from card where node_id = <node-id> and slot =
<slot-num> " | dbaccess
```

The fc_state of the card must be 3.

Defect Information—Collect the following information for further analysis:

- Pmcollector.log, output of:

```
echo "select fc_state, fc_type, slot from card where node_id = <node-id> and slot =
<slot-num> " | dbaccess
```

- Related key index entries
- Pmcollector

Possible alternative workaround—If the card is not in fc_state 3, look up troubleshooting for the EM module.

J.10.10.1.4 PM Collection Fails for the Node—Log File Shows "Time not synchronized"

This can happen when the time stamp between the CTM and the collector is not synchronized or the time stamp between the collector and the node is not synchronized.

Step 1 Check the sync_info table by executing the following command:

```
echo "select offset from sync_info where sync_node_id=<node_id>" | dbaccess
```

Step 2 Check the time on the CTM/Collector and on the node and make sure the offset from the previous query is the difference of time in seconds.

Step 3 For feeders, check the time difference between CTM and the routing node of the feeder.

Defect Information—Collect the following information for further analysis:

- Pmcollector.log
- Related key index entries
- Pmcollector

Possible alternative workaround—Set the time on the CTM/Collector and the node to the same time stamp.

J.10.10.1.5 PM Collection Fails for the Node—Log File Shows "Snmp failed"

This can happen due to SNMP failure caused by an incorrect community string or a timeout.

Step 1 Check get_str and set_str in the node_info table and make sure they are the community strings on the node. Check the SNMP community strings on the node using the command **dspsnmp**.

Step 2 To check the log files for more details on the error, grep "snmp" scm*. If the error is a timeout error, change the timeout setting and retry the setting in /opt/svplus/config/pmcollector.conf.

Defect Information—Collect the following information for further analysis:

- Pmcollector.log
- Related key index entries
- Pmcollector, manual SNMP results

Possible alternative workaround—If the community strings are different on CTM and the node, look up troubleshooting for the Topology module.

J.10.10.1.6 PM Collection Fails for the Node—Log File Shows "Ftp failed"

This could happen for various reasons; generally, it is because of an incorrect username/password or a timeout.

Step 1 Check the node_id, node_name, and IP address in the node_info table and make sure they are the correct ones.

Step 2 Check the type of IP routing used while starting collection. Verify whether the IP address used in the IP routing is reachable or valid.

Step 3 Verify that the ftp_user_name and ftp_user_passwd in the coll_info table and the ftp_user_name and ftp_user_passwd in the node_info table of the stratacom database are matching and are valid.

Defect Information—Collect the following information for further analysis:

- Pmcollector.log, dump of coll_info table, dump of node_info table of stratacom
- Related key index entries
- Pmcollector

Possible alternative workaround—Use the atm or LAN IP that is reachable.

J.10.10.1.7 PM Collection Fails for the Node—Log File Shows "Polling failed and wait for major retry" or "Major retry failed and wait for critical retry" or "Critical retry failed and wait for history retry" or "History retry failed and wait for next retry" or "No more retry"

This could happen for various reasons, but it is mainly due to ftp/tftp failures.

Step 1 Verify that the node is reachable (pingable) with nw_ip_address or lan_ip_address.

- If only the nw_ip_address is reachable and the lan_ip_address is unreachable, then make sure that IP Routing for stats collection is using In Band.
- If only the lan_ip_address is reachable and the nw_ip_address is not reachable, then make sure that IP Routing for stats collection is using Out of Band.
- Use the **dspifip** command to check the lan_ip_address and nw_ip_address.

Step 2 Check the pmcollector.log to verify whether or not you are using the correct ip_address for stats collection.

Step 3 Check for the existence of connections on the slot for which you are collecting the stats. Also check for the stats' flag. Use the command **sumDBShow** or **sfmDBShow** on the node.

Step 4 Verify that the ftp_user_name and ftp_user_passwd in the coll_info table and the ftp_user_name and ftp_user_passwd in the node_info table of the stratacom database are matching and are valid.

Defect information—Collect the following information for further analysis:

- Pmcollector.log, dump of node_info and coll_info
- Related key index entries
- Pmcollector

Possible alternative workaround—Use the atm or LAN IP that is reachable.

J.10.10.2 PM Parsing Issues

This section includes the following information:

- J.10.10.2.1 StatsParser—Generic Troubleshooting, page J-121
- J.10.10.2.2 StatsParser—Files Are Parsed But the Files Are Listed in the BadFileList, page J-121

J.10.10.2.1 StatsParser—Generic Troubleshooting

StatsParser reads the data from the stat files and inserts the data into the database.

When performing generic troubleshooting, always do the following:

Step 1 Verify that the statsparser process is running by executing the **psg statsparser** command and checking for a result.

Step 2 Check the log level for the statsparser. You can increase the log level by editing the config file ~/config/statsparser.conf and changing the value in the LOG_LEVEL field to 7.

J.10.10.2.2 StatsParser—Files Are Parsed But the Files Are Listed in the BadFileList

While parsing the stats files and inserting the data into the database, if the StatsParser encounters a problem with the parsing of data in the stats file or a problem with the format of the file, the file is put in the BadFileList.

The node entry is not available in the scmnode table. Perform the following query and verify whether:

- All the nodes that are in the Collection state are listed in the output. Also, determine whether:
  - Node entries are duplicated. The query is:

    % echo " SELECT * from scmnode" | dbaccess
  - The file is corrupted. Read the file manually using the statsreader:

    % statsreader <stats filename>

    Note If the output doesn't look normal or the file looks corrupted, then the problem is most probably on the switch side. Report the problem to the CTM team and the switch team.
- There is space left on the machine to insert any more. If not, report the problem immediately.

Defect Information—Collect the following information for further analysis:

- Statsparser.log, output of df -k and mount
- Related key index entries
- BadfileList

J.10.11 Statistics Report Problems

This section includes the following information:

- J.10.11.1 Statistics Report, page J-122
- J.10.11.2 You Collected Data but You See No Data Available, page J-122

- J.10.11.3 You Generated a Report but Do Not See Data for a Long Time, page J-122
- J.10.11.4 You See FDNs for Other Entities when You Generate a Report, page J-122
- J.10.11.5 You See the Wrong FDN for a Raw Report, page J-122
- J.10.11.6 Utilization Report Value Is Greater than 100%, page J-123

J.10.11.1 Statistics Report

You can use the Statistics Report to view reports of statistics data that are collected from the switch.

The SRT GUI provides the ability to generate and view historical statistics reports. Reports such as Raw Statistics and Top Utilization are shown in table format and performance data reports are shown in graph and table formats.

J.10.11.2 You Collected Data but You See No Data Available

Step 1 Verify that the data has been collected and parsed.

Step 2 Verify that the corresponding table has data for the specified time period.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None.

J.10.11.3 You Generated a Report but Do Not See Data for a Long Time

If you are trying to generate reports and you don't see any data for a long time and you only see the message Retrieving data, check srtserver.log for any error messages.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None.

J.10.11.4 You See FDNs for Other Entities when You Generate a Report

When you generate a raw report for trunk data on one card, you might also see trunk data from a different card. This is because some of the tables do not have slot information and hence you get data only with node information.

This is not an error. You will see extra data.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None.

J.10.11.5 You See the Wrong FDN for a Raw Report

The FDN reported is contains either wrong values or junk values.

This is an error on the server while forming FDN.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None.

J.10.11.6 Utilization Report Value Is Greater than 100%

The Utilization report value is greater than 100%.

This is an error.

Defect Information—Collect the following information for further analysis:

- /opt/svplus/log/srtserver.log

Possible alternative workaround—None.

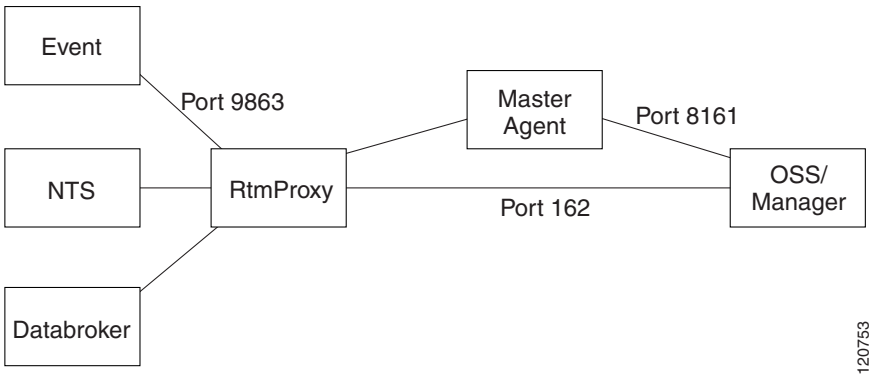
J.10.12 Service Agent Problems

RtmProxy is the only component in the Service Agent that is used in CTM. The Service Agent processes your requests through SNMP, convey them to the switch agent, and finally returns the result to you.

J.10.12.1 RtmProxy

RtmProxy is CTM's northbound SNMP interface, providing traps from all switches to customer applications. It is an interface with which the customer application registers for traps. The customer application uses SNMP to register with RtmProxy. Figure J-7 shows the flow of information.

Figure J-7 RTMProxy



The OSS/Manager send an SNMP request to port 8161 of the CTM machine. In this request, the OSS/Manager specify the port on which OSS/Manager are listening for. In the above example, the Manager is sent traps on port 162. The registration, deregistration, and other such scripts can be found at /opt/svplus/scripts/proxyscripts/rtmproxy on a CTM machine. These scripts can be used for reference for registration and deregistration with RtmProxy. These scripts are meant only for internal use.

J.10.12.1.1 Registration with RtmProxy Failed

Manager's SNMP request to register with RtmProxy returned an error.

Step 1 Verify that the CTM core is up and running by executing **ps -ef | grep RtmProxy** on the CTM machine.

Step 2 Verify that the snmpset request was sent to port 8161.

Step 3 Verify that the community string for the snmpset is set to private.

Step 4 Verify that the MIB objects that are being set are correct.

The MIB objects that should be set for the Manager's registration are:

- stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerRowStatus
- mstratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.trapFilterRegisterCategory
- stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerPortNumber

Step 5 Verify that the IP address to which you are sending the snmpset request is correct.

Defect Information—Collect the following information for further analysis:

- RtmProxy.log* and snmpd.log*

Possible alternative workaround—None.

J.10.12.1.2 Not Receiving Any Traps

Traps are not being received on the port with which the Manager registered.

Step 1 Verify that the registration with RtmProxy went through successfully. If the registration did not go through, see J.10.12.1.1 Registration with RtmProxy Failed, page J-124.

Step 2 Use the following to verify that the port number that RtmProxy is sending traps to is the same as the port number on which the trap receive utility or Manager is listening.

```
tballraker29% /opt/OV/bin/snmpget -d -v1 -p8161 -t 3000 -r 0 -cpublic 172.28.131.137
stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerPortNumber.172.28.131.158
```

where 172.28.131.137 is the CTM IP address and 172.28.131.158 is the Manager IP address (or IP address of the station where the trap receive utility is running).

Step 3 Use the following to verify that the Manager is still registered with RtmProxy.

```
tballraker29% /opt/OV/bin/snmpget -d -v1 -p8161 -t 3000 -r 0 -cpublic 172.28.131.137
stratacom.rtm.trapsConfig.trapConfigTable.trapConfigEntry.managerRowStatus.172.28.131.158
```

where 172.28.131.137 is the CTM IP address and 172.28.131.158 is the Manager IP address (or IP address of the station where the trap receive utility is running).

The SNMP should return 1.

Defect Information—Collect the following information for further analysis:

- RtmProxy.log* and snmpd.log*

Possible alternative workaround—Reregister with RtmProxy.

J.10.12.1.3 Manager Gets Deregistered

The Manager is deregistered from RtmProxy after running for a while.

Step 1 Verify that the keepalive script is running. The Manager will automatically get deregistered if no SNMP is done on any of the tables in RtmProxy. To keep the Manager registered with RtmProxy, run the keepalive script in the background, as follows:

```
#!/bin/sh
Usage="$0 <Agent Ip Address> <Manager IP address>"
if [ $# -lt 2 ]
then
echo "Usage :$Usage"
exit 1
fi
managerRowStatus=.1.3.6.1.4.1.351.120.1.1.1.3
managerPortNumber=.1.3.6.1.4.1.351.120.1.1.1.2
lastseq=.1.3.6.1.4.1.351.120.1.3.0
while true
do
sleep 60
CMD="/opt/OV/bin/snmpget -cpublic -p8161 -t3000 -r0 $1 $managerRowStatus.$2 $lastseq"
echo $CMD
$CMD
done
exit 0
```

Step 2 Verify that IP reachablity the CTM station is not lost of from the station where the Manager is running.

Defect Information—Collect the following information for further analysis:

- RtmProxy.log* and snmpd.log*

Possible alternative workaround—Reregister the Manager with RtmProxy.

J.10.12.1.4 Nodal Community Strings Do Not Work

Snmpwalk using the nodal community strings returns an error.

Step 1 Verify that the SNMP request is being issued to port 8161.

Step 2 Verify that the community string is correct.

Defect Information—Collect the following information for further analysis:

- RtmProxy.log* and snmpd.log*

Possible alternative workaround—None.

J.10.12.2 Audit Trail Logging Mechanism Problems

Audit trail logging provides CTM with the ability to record user activities across different modules in a persistent file. All CTM Java front GUI applications send information about user activities to the Audit Logger server through the CORBA interface. The Audit Logger server then writes the data into the persistent log file.

This section includes the following information:

- J.10.12.2.1 AuditLogger.conf Usage, page J-126
- J.10.12.2.2 Audit Trail Log File Naming Convention, page J-126
- J.10.12.2.3 When You Open a Dialog Box in a CTM GUI, There Is No Record in the Audit Trail Log File, page J-126

J.10.12.2.1 AuditLogger.conf Usage

The following can be configured in the configuration file:

- Location of the log file—The default is (/opt/svplus/log/AL).
- Number of days—By defining the number of days for the audit trail log files to be kept, all other obsoleted audit trail logs will be deleted automatically.
- The name of the user group whose member can read the audit trail log files—It is a standard UNIX user group.

J.10.12.2.2 Audit Trail Log File Naming Convention

There is one audit trail log file per day. The filename convention is defined as AuditTrail.<mmddyyyy>.log.

Example audit trail log files: AuditTrail.10102001.log for October 10, 2001.

J.10.12.2.3 When You Open a Dialog Box in a CTM GUI, There Is No Record in the Audit Trail Log File

Step 1 Open the CTM Security Manager GUI, and check the Audit-Read permission for that CTM GUI in the security profile associated with the user. If the Audit-Read permission is not turned on, then no record is the expected behavior. Otherwise, go to step 2.

Step 2 Verify that the Audit Logger server is running. Use **psg AuditLogger** on the CTM machine. If no AuditLogger server is running then this is the problem. Go to defect information and follow the steps to collect all the information needed.

Step 3 Check to see if any CORBA-related exceptions have been thrown on the console. If so, collect those error messages and/or call stacks.

Defect Information—Collect the following information for further analysis:

- Complete screen snapshots of the CTM GUI.
- Errors/exceptions thrown on the console, if any.
- log: /opt/svplus/log/AuditLogger.log*, /opt/svplus/log/LogServer.log*, AuditTrail*.log (file location is set in /opt/svplus/config/AuditLogger.conf), /opt/svplus/log/watchdog.log.
- Core dump files in /opt/svplus/corefilesdir, especially for those AuditLogger core dump files.

J.10.13 Miscellaneous Problems

This section includes the following information:

- J.10.13.1 NTS, page J-127

- J.10.13.2 Data Inconsistency, page J-129
- J.10.13.3 CTM FTP Daemon, page J-134

J.10.13.1 NTS

This section includes the following information:

- J.10.13.1.1 Nodes Stay in Mode 1 After ColdStart, page J-127
- J.10.13.1.2 Config Change or Provisioning Activity Not Reflected on CTM, page J-127
- J.10.13.1.3 How To Interpret NTS Log, page J-128

J.10.13.1.1 Nodes Stay in Mode 1 After ColdStart

The nts cannot manage a particular switch successfully. In other words, nts declared the switch to be in the Unreachable or Unregistered state. As a result, nts notified its clients with a LINK_DOWN message. The nts declares a node to be in OK state if it is in the Trap Manager List of the node and can successfully perform SNMP operations on the node.

Step 1 Check the PING reachability. Run **ntsControl** and enter **ni** at the prompt. Then, enter **q** to exit ntsControl. This shows the nts node information. A node has to be in OK state so that CTM can start syncing it up. If the node is not in OK state, first thing to check is PING. Run **ping <ip_address>**. If the PING succeeded, go to step 2. Otherwise, fix the network reachability between the switch and the CTM station.

Step 2 Check the CTM IP address configuration This only applies to CTM workstation with multiple IP interfaces. The NMS_IP_ADDRESS setting in /opt/svplus/config/svplus.conf has to match the interface users chose for CTM. To check the IP interfaces, run **ifconfig -a**. CTM stations with only one IP interface does not need to have the NMS_IP_ADDRESS setting.

Step 3 Check the Trap Manager List on the switch. SSH or Telnet to the switch. Run **dsptrapmgr** command to show the Trap Manager List. Check whether the CTM is in the table. If so, go to step 4. Otherwise, if the table is already full, remove unwanted entries with **deltrapmgr** command. The nts should be able to register the CTM into the table within a few minutes. If not, go to step 4.

Step 4 Check the SNMP community strings. In case the SNMP community string on the switch has been changed from the default setting, the SNMP community string on the CTM have to match the new ones on the switch. The SNMP community string on the switch can be viewed with **dspsnmp** command. The setting on the CTM can be viewed in Domain Explorer.

Defect Information—Collect the following information for further analysis:

- Selnd and dbnds command output
- Nts log and EM log of the node in question.

Possible alternative workaround—If community strings do not match, run the CTM Configurator GUI to correct them. (/opt/svplus/java/bin/runConfigurator)

Related key index entries: nts, traps

J.10.13.1.2 Config Change or Provisioning Activity Not Reflected on CTM

The nts does not receive any traps from a particular switch when it actually had generated traps.

Step 1 See if the node is in OK state. If the ntsControl node information says the particular node is not in the OK state, see J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129. If the node is indeed in OK state, go to step 2.

Step 2 Check the Trap IP address setting on the switch. The Trap IP address has to be the primary IP address of the switch. Otherwise, nts cannot correlate the trap with the CTM node information and has to discard that trap. SSH or Telnet to the switch. The primary IP address can be found with **dspndparms** and then **dspifip** commands. Enter **dsptrapip** to see the current Trap IP address setting. Use **cnftrapip** to correct. See J.10.13.1.3 How To Interpret NTS Log, page J-128 for more information.

Defect Information—None.

Possible alternative workaround—None.

Related key index entries: nts, traps

J.10.13.1.3 How To Interpret NTS Log

Locating a specific trap from a particular node in the nts log.

Step 1 Verify trap handling.

The nts log has information on the traps delivered to a specific client. The nts, by default, keeps 20 old logs in addition to the current one. You can form your **grep** command with the key fields such as node ID, trap number, client name, and pid. For example:

```
( 21359: 63) 19:24:40 WARNING: N42 Trap(6, 50017, #15668881) to EMC-5-24596
```

The above line says nts delivered Node 42 Trap 50017 Sequence Number 15668881 to EMC child 5 PID 24610.

In normal case, you see the following cluster for each trap in nts log:

```
( 21359: 46) 01:46:49 WARNING: N15 Trap(6, 60303, #25278)
( 21359: 46) 01:46:49 WARNING: N15 Trap #25278 buffered
( 21359: 48) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to CSA
( 21359: 50) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to RtmProxy
( 21359: 60) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to ooemc-24610
( 21359: 58) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to EMD
( 21359: 49) 01:46:49 WARNING: N15 Trap(6, 60303, #25278) to HPOV
```

where:

- Line 1 means "Trap(6, 60303, #25278)" is received by nts
- Line 2 means it is successfully buffered by nts
- Lines 3 to 7 mean it is delivered to the clients who registered to receive it in their XML filter setting

Step 2 If you cannot find the particular trap, verify if the switch is sending traps with a wrong trap IP address. If the switch trap IP is wrong, traps from it is declared as coming from unmanaged node and dropped. The Trap IP address has to be the primary IP address of the switch. Otherwise, nts cannot correlate the trap with the CTM node information and has to discard that trap. See J.10.13.1.2 Config Change or Provisioning Activity Not Reflected on CTM, page J-127 for more information.

The nts prints a different message when a trap comes from a node it does not yet manage (unknown node_id), for example:

```
nts.7275.log.old.2:( 7275: 45) 03:32:39 WARNING: Trap unmanaged 172.28.140.16
```

In that case, it prints the IP address only and throw it away.

Defect Information—None.

Possible alternative workarounds—None.

Related key index entries: nts, log

J.10.13.2 Data Inconsistency

This section includes the following information:

- J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129
- J.10.13.2.2 Inconsistent Connection Status, page J-132
- J.10.13.2.3 Inconsistent Connection Secondary Status, page J-132
- J.10.13.2.4 Incomplete Connections, page J-133

J.10.13.2.1 Connection Inconsistency Between the Switch and GUI

This section discusses strategies for debugging inconsistencies between the switch and the CTM GUI. The inconsistencies discussed in this section are not directly related to provisioning. The problems may be caused by coldstart, warmstart, or provisioning, but they are noticed sometime after the fact; for example, you might look at the system and suddenly realize there is an inconsistency.

This section gives a list of steps to try to determine more precisely the cause of the inconsistency. These steps should be performed in order:

1. Verify the node's sync states
2. Isolate the connection inconsistency by using a database query
3. Isolate the connection inconsistency by using a message flow

Step 1 Check the node’s state after startup. If the node is in an abnormal state, it can result in incorrect counts or the presence of incomplete connections.

a. Determine if sync-up has been completed.

b. If the system has declared sync-up, use the CTM CLI command **selnd** to verify that the nodes on which you see the inconsistency are in mode 3. The second-to-last column identifies the mode for a given node.

Step 2 Check the user_connection table and the segment tables for problems. The information displayed on the Connection Manager GUI is taken directly from the user_connection table. The Connection Manager is rarely the problem. This procedure uses database access queries to help isolate the problem. If the problem is found in the user_connection table and the segment tables are incorrect, the problem is usually in the EM. If the user_connection table is wrong but the segment tables are correct, you will need to continue with the investigation before you can determine a root cause.

Note All ports in the database and the messages are 0-based, and all ports on the switch CLI are 1-based. Therefore, if the switch shows port 3, then you should query for port 2.

a. Query the user_connection table for one of the connections in question. For example, if the connection has a local endpoint of node = n, slot = s, logical port = p, vpi/dlci = s1, vci = s2, then the query would look like this:

```
SELECT * from user_connection where l_node_id = n, l_slot = s, l_logical_port = p,
l_subchnl_1 = s1, l_subchnl_2 = s2
```

If you are unsure which side is local and which is remote, try a query with both l_node_id = n and r_node_id = n (and slot, port, and so on). If this row in the database is inconsistent with the same information on the switch, more investigation is required.

b. Verify that the databroker has received all traps from the EMs. To do this, view the columns inseg_tbl_1, inseg_tbl_2 and inseg_tbl_3. If the flag is set to '1' then all traps for the given segment have been received. A flag tells you if the databroker received an add message for the given segment. If it is set to 0 it means the segment trap has not been processed by the databroker. If the flag is set to 2 or 3, that means only one end of the segment has been processed.

Note If the connection does not have three segments, the unused segments default to 1.

c. You should now check the EM connection tables for the connections in question. If you see that the segment tables are correct and the user_connection table is not, or if the inseg_tbl_x flags are not all = '1', you should continue testing, see J.10.13.2.2 Inconsistent Connection Status, page J-132. If you see that the segment tables are also incorrect, go to step 3.

Step 3 In some cases a more detailed review of the message flow between EM, DMD, and sdbroker is necessary to determine the source of the error:

a. Verify that DMD received the message from EM. Search the message log for the connection. This search is on the DMD first, followed by the sdbroker and xdbroker (xpvc only). The search is either by connection object ID or node/slot/port/vpi/vci. The DMD logs are checked, and if no messages are found, then the ooemc or other EM processes are checked. If the message is found, or the logs are incomplete, then you need to look deeper into the databroker processes. If the DMD or the EM logs are complete and the message was not sent to DMD, then it is most likely an EM issue.

Find the DMD by using the command /opt/svplus/dbcmap -d <node_id>. The output will provide you with the DMD whose logs need to be queried.

```
grep "node <node_id> slot <slot #> .* port <logical_port> .* sCh1 <vpi or dlci> sCh2
<vci>" dmd<dmd_id #>Msg*
```

Each output line is similar to this:

```
( 7) 21:49:43 1058910582 MsgType=100 connObjId 65665 connStatus 1 secStatus 1
upperLevelAlrm0 oamStatus 0 channelNo -4272512 termination 1 masterFlag 0 wildCardFlag
0 controllerType 0 subType 55 lPercUtil 100 rPercUtil 100 persistentSlave 1
prefRouteId 0 directRouteFlag 0 Local node 11 slot 15 line -1 port 0 logPort 0 sCh1 1
sCh2 37 type 1 subType 0 nni -1 netprefix Remote node 11 slot 14 line -1 port 0
logPort 0 sCh1 32 sCh2 234 type 1 subType 0 nni 0 netprefix
```

Items of interest in the above example are:

21:49:43—The time at which the event occurred.

Local node11 slot 15 .... sCh1 1 sCh2 37—The local endpoint.

Remote node 11 ....—The remote endpoint.

MsgType=100—The message type. The mapping is as follows:

FEEDER_ADDUPD = 100,

MASTER_SPVC_ADDUPD = 101,

SLAVE_SPVC_ADDUPD = 102,

SINGLEENDSPVC_ADDUPD = 103,

PTOMPSPVC_ADDUPD = 104,

MASTER_PVC_ADDUPD = 105,

SLAVE_PVC_ADDUPD = 106,

MASTER_LOCALDAX_ADDUPD = 107,

SLAVE_LOCALDAX_ADDUPD = 108,

FEEDER_DEL = 109,

MASTER_SPVC_DEL = 110,

SLAVE_SPVC_DEL = 111,

SINGLEENDSPVC_DEL = 112,

SLAVE_SPVC_DEL = 111,

SINGLEENDSPVC_DEL = 112,

PTOMPSPVC_DEL = 113,

MASTER_PVC_DEL = 114,

SLAVE_PVC_DEL = 115,

MASTER_LOCALDAX_DEL = 116,

SLAVE_LOCALDAX_DEL = 117,

WILDCARD_DEL = 121,

grep conObjId xxxxxx dmd<dmd_id>Msg*

grep <NotifyDataBroker> .*node x slot y .* sub1 v sub2 w ooemc* < for more EM queries see EM>

b. If the DMD received the message but it is not reflected in the database, identify which databroker module caused the error. First check the DMD to see if it forwarded the message. If it did not check for the reason. The format may be wrong or there could be other similar problems. Try to search/ grep node/slot/port/vpi/vci. This is output every time a cache query is done.

grep "DROP MSG: validation error" dmd<dmd_id>.<pid>.* - prints out dropped messages.

c. If the message made it to DMD, you need to see if the sdbroker received the message.

grep "node <node_id> slot <slot#> .* port <logical port> sCh1 <vpi/dlci> sCh2 <vci>" sdbroker*Msg*

d. If it looks like the message was received by the sdbroker but the database does not reflect the change, then you should verify if there is an inconsistency between the databroker cache and the database. To dump the cache, enter:

```
$ psg sdbroker
```

The process ID of the sdbroker will be returned.

```
$ kill -USR1 <process ID returned from the previous command>
```

The cache dump will be written to a file in /opt/svplus/log/sdbkrCache.dump. Verify if the connection in question is correct in the cache.

Defect Information—You need the logs of the processes on both sides of the interface on which the message was dropped. A dump of the specific user_connection table entry that is incorrect is also useful as well as the segment tables for this connection. The specific node, slot, logical_port, vpi, and vci of both ends of the connection in question is also useful. If a cache dump was done, include that also.

Possible alternative workarounds—If the problem is between the sdbroker cache and the database, a cache resync can be done. To do this execute the command /usr/usrs/svplus/tools/CacheResync [-t <time in seconds>]. If the problem still exists, collect the defect information.

Related key index entries: inconsistency, connection, databroker

J.10.13.2.2 Inconsistent Connection Status

The GUI display of Status is from the state field of the user_connection table. The field represents the worst condition of any of the segments in the connection. This field values are:

- 1 = Clear
- 2 = Fail
- 3 = Down
- 4 = Incomplete
- 5 = Error

Step 1 If the value is not what is expected, check the connection level databases for each segment to see if they are correct.The last message on the segment in question is the important one.

Step 2 If the status is incomplete it means that one of the segments of the connection is not in the user_connection table, check the in_seg flags in the user_connection table entry for this connection. Search the database and messages for the segment that has flag = 0.

If two primary endpoints each have the same secondary endpoint, then you have an errored connection. The first connection established will have a status of Error and the second primary endpoint connected to the secondary will have a status of Incomplete.

Defect Information—See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129.

Possible alternative workaround—See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129.

Related key index entries: inconsistency, connection

J.10.13.2.3 Inconsistent Connection Secondary Status

The GUI display of Secondary Status is from the Secondary_status field of the user_connection table. The field represents the worst condition of any of the segments in the connection. This field is a bit map with each secondary status using 2 bits. The values of each status entry are:

- 0 = unknown
- 1 = ok

- 2 = fail

The bit pattern is:

- Bits 1, 2—Local abit
- Bit 2, 4—Local AIS
- Bit 5, 6—Local OAM
- Bit 7, 8—Local Conditioned
- Bit 9, 10—Remote abit
- Bit 11, 12—Remote AIS
- Bit 13, 14—Remote OAM
- Bit 15, 16—Remote Conditioned

Step 1 If the value is not what is expected, check the connection level databases for each segment to see if they are correct. See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129. The last message on the segment in question is the important one.

Defect Information—See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129.

Possible alternative workaround—See J.10.13.2.1 Connection Inconsistency Between the Switch and GUI, page J-129.

Related key index entries: inconsistency, connection

J.10.13.2.4 Incomplete Connections

A common issue is having too many connections on a given card. This problem may be a result of incomplete connections. For example, if a feeder segment of a three-segment connection has not been processed by the databroker, the incomplete connection will have an endpoint of a routing node, not the missing feeder. There will appear to be too many connections on the routing node. A connection can be identified as incomplete if the state is equal to four in the user_connection table.

Step 1 Check the user_connection table for the number of segments and the inseg flags for the connection in question.

Step 2 Select num_segs, status, inseg_tbl_1, inseg_tbl_2, inseg_tbl_3 from user_connection where l_node_id = x and l_slot=y and l_port=z and l_subchnl_1 = v and l_subchnl_2 = w.

Defect Information—You need the logs of the processes on both sides of the interface on which the message was dropped. A dump of the specific user_connection table entry that is incorrect is also useful. The specific node, slot, logical_port, vpi, vci of both ends of the connection in question is also useful.

Possible alternative workarounds—If the problem is between the sdbroker cache and the database, a cache resync can be done. To do this execute the command /usr/usrs/svplus/tools/CacheResync [-t <time in seconds>].

Related key index entries: inconsistency, incomplete connection

J.10.13.3 CTM FTP Daemon

This section includes the following information:

- J.10.13.3.1 FTP Daemon Overview, page J-134
- J.10.13.3.2 Generic Troubleshooting, page J-134
- J.10.13.3.3 FTP Username and Password, page J-134
- J.10.13.3.4 cwmftpd—Files Are Not Transferred Due to Wrong Username/Password, page J-135
- J.10.13.3.5 cwmftpd—File Not Available On Switch, page J-135
- J.10.13.3.6 FTP Sessions in Switch, page J-135
- J.10.13.3.7 421 Session Limit Reached, page J-136
- J.10.13.3.8 499 Session Limit Reached, page J-136
- J.10.13.3.9 Failed to Acquire a Session with a Switch, page J-137
- J.10.13.3.10 Failed to Acquire Session After All Retries, page J-137
- J.10.13.3.11 General Log Information, page J-137

J.10.13.3.1 FTP Daemon Overview

The cwmftpd process is an ILOG server that allows CTM modules to request an FTP put, get, or directory listing service to and from network nodes or other CTMs. This server acts as an FTP client from an FTP communication standpoint and performs services similar to the interactive ftp program.

The following processes use cwmftpd to FTP the files:

- ooemc
- PM collector

Related key index entries: FTP

J.10.13.3.2 Generic Troubleshooting

When performing generic troubleshooting, always do the following:

- Check whether the cwmftpd process is up and running.

  ```
  psg cwmftpd
  ```

- Check the free disk space.

  ```
  df -k /opt/svplus
  ```

- Check whether target switch/CTM is reachable.
- Check for debug level. If logs are not giving detailed information, debug level can be increased by editing ~svplus/config/cwmftpd.conf.
- Set the config parameter, LOG_LEVEL, to 7 to get detailed logs.

Related key index entries: FTP

J.10.13.3.3 FTP Username and Password

The command **cwmftpd** uses the node_info table of the stratacom database to retrieve the FTP username and password. For SCM requests, scmcollsvr sends the password along with the request.

Related key index entries: FTP, username, password

J.10.13.3.4 cwmftpd—Files Are Not Transferred Due to Wrong Username/Password

Files are not transferred between CTM and the switch or between CTMs due to a wrong username/password.

The files are not FTP'd between the switch and CTM or between CTMs due to a wrong FTP username/password.

Step 1 Check whether the FTP username and password are correct.

Step 2 Check whether cwmftpd.log is having an exception like the following, where the FTP username and password are wrong:

```
(22589:204248) 10:12:27 ERR: %FtpException-3-LOGIN_FAILED: Login failed.
[login,host=172.23.30.111,user=superuser]
```

Defect Information—If username/password are correct, but LOGIN_FAILED is still shown in logs, collect cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Related key index entries: login failed

J.10.13.3.5 cwmftpd—File Not Available On Switch

A file is not transferred because it is not available.

Step 1 Check whether the file is available in the target switch.

Step 2 Check whether cwmftpd.log contains an exception like this:

```
FtpException-3-FTPERR_550: Requested action not taken. File unavailable (e.g., file not
found, no access). [550 File "/stat/1-05-Con-062020031215" not found or permission
problem]
```

Defect Information—If the file is available but was not FTP'd, and an FTPERR_550 exception is thrown, then collect cwmftpd.log, cwmftpd.request_log and logs of the process for which the file was not transferred by cwmftpd and report the problem.

Possible alternative workaround—None.

Related key index entries: file unavailable, ftperr_550, requested action not taken

J.10.13.3.6 FTP Sessions in Switch

A switch allows only four FTP sessions. When cwmftpd makes a request to open a session, if the switch cannot service the request because it has reached its session limit or if the file is locked, then the switch will respond with the following error message "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>."

Key is a unique string for the node, which is used later when the session is available. CTM waits on a TCP Port 5120 for the switch to connect to. When a session is available, the switch connects to the predefined port and sends the key as data to CTM. CTM uses the key to identify which switch it needs to open the session with. The session should now be opened without encountering a failure and cwmftpd can proceed with the FTP request.

The switch will reserve the session for the CTM station for 30 seconds before it services other stations. CTMftpd will retrieve multiple files within a single FTP session. A maximum limit per session will be imposed.

This feature is supported in CTM with MGX 8850 Release 4.0 or later. For Switch Software (SWSW) earlier than MGX 8850 Release 4.0, the switch responds with "421 Session limit reached, closing control connection."

The number of FTP sessions currently opened by the switch can be determined by executing the switch command **dsptasks**. For each FTP session, dsptasks output will have an entry like following:

```
FtpdServ1 0x9a00a1 0x82d8a8a0
```

If there are two sessions, there will be two entries.

Related key index entries: switch FTP session

J.10.13.3.7 421 Session Limit Reached

For SWSW earlier than MGX8850 Release 4.0, the switch responds with "421 Session limit reached, closing control connection," when it reaches the limit of four FTP sessions.

Step 1 Check whether all four sessions have been opened by opening a manual FTP session to the switch or by executing the switch command **dsptasks**.

Defect Information—If manually opening the FTP session succeeds or the **dsptasks** command shows less than four entries for FtpdServ, but **cwmftpd** still throws FTPERR_421, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Possible alternative workaround—None.

Related key index entries: service not available, closing control connection, 421, session limit reached, ftperr_421

J.10.13.3.8 499 Session Limit Reached

For SWSW MGX8850 Release 4.0 or later, the switch responds with "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>," when it reached the limit of four FTP sessions.

The **cwmftpd** command will throw the exception FTPERR_499, when it tries to connect to a switch which responded with the error, "499 Session limit reached, queuing <IP address> key <Nodename/XXXXXXXX>."

Step 1 Check whether all four sessions have been opened by opening a manual FTP session to the switch or by executing the switch command **dsptasks**.

Defect Information—If manually opening the FTP session succeeds or the **dsptasks** command shows less than four entries for FtpdServ, but **cwmftpd** still throws FTPERR_499, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Related key index entries: 499, session limit reached, key, ftperr_499

J.10.13.3.9 Failed to Acquire a Session with a Switch

For MGX 8850 Release 4.0 or later, CTM waits in a predefined port to acquire the session, if it receives the "499 Session limit reached" error. This wait time is 1 minute by default and is configurable. If CTM does not get a response from the switch within this wait time, it times out and throws the following exception and then again retries to open the session:

```
( 9583: 6) 08:37:29 ERR: %CwmFtpDaemonException-3-SESSION_TIMEOUT: Session [Id[28],
ClientSeq#[6521], Host[172.25.69.218], User[superuser], Priority[3]:get
/stat/1-04-Con-052920030730 /opt/svplus/spool/MGX98101-1-04-Con-052920030730-2] timeout in
3 minutes and needs to be retried.
```

It retries 5 times by default (this number is configurable). If all retries fails, cwmftpd throws the following exception:

```
( 9583:172473) 08:37:58 ERR: %CwmFtpDaemon-3-SESSION_FAIL: Thread [Host [172.2
5.69.218] User[superuser] NoRequest] failed to acquire session after 5 retries. Session
wait time[5].
```

Related key index entries: switch, session, FTP

J.10.13.3.10 Failed to Acquire Session After All Retries

The **cwmftpd** command failed to acquire a session with a switch on all retries.

Step 1 Check whether all four sessions have been opened by opening a manual FTP session to the switch.

Defect Information—If manually opening the FTP session succeeds, but cwmftpd still throws a SESSION_FAIL exception, then report the problem with cwmftpd.log, cwmftpd.request_log and logs of the process for which files are not getting transferred by cwmftpd.

Possible alternative workaround—None.

Related key index entries: session_timeout, session_fail

J.10.13.3.11 General Log Information

The cwmftpd.request_log file will have one entry for each request. It will have information about whether the request succeeded or failed and how much time it took. It has information in a short and simple format and since there is not much data per request, the file has more data in terms of amount of time.

Cwmftpd maintains information based on the IP address of the node. To track a request for a particular node, grep for the IP address as the keyword in cwmftp.log and cwmftpd.request_log.

When ooemc sends FTP requests, it also sends the node ID along with the request as part of the destination file. This node ID is used to retrieve the FTP user/password from the node_info table. This can be used for user/password validation.

The following keywords are from the cwmftpd.log file.

- TRANSFER_STARTED—Specifies that cwmftpd started transferring the file.
- TRANSFER_COMPLETED—Specifies that the file has been transferred completely and also gives information about local and remote file size.
- TRANSFER_RATE—Specifies the rate of transfer with the number of bytes transferred and the time.

- TRANSFER_RETRY—Specifies that the transfer request needs to be retried.
- TRANSFER_FAILED—Specifies that cwmftpd was unable to transfer the file.
- CONTROL_CONN_TIMEOUT—This exception will be thrown where there is no transfer of information for X seconds once the FTP session is opened.

Related key index entries: FTP log